CÁC PHỤ LỤC HƯỚNG DẪN THIẾT LẬP QUY TẮC CẤU HÌNH ATTT

(Được ban hành theo Bộ quy tắc cấu hình ATTT cho các hệ thống thông tin)

Phụ lục 01. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HĐH WINDOWS CỦA NGƯỜI DÙNG CUỐI 2

Phụ lục 02. HƯỚNG DẪN LẬP TRÌNH AN TOÀN TRONG PHÁT TRIỂN ỨNG DỤNG WEB TRÊN FRAMEWORK .NET 41

Phụ lục 03. HƯỚNG DẪN LẬP TRÌNH AN TOÀN SỬ DỤNG ỨNG DỤNG C/C++ 66

Phụ lục 04. HƯỚNG DẪN LẬP TRÌNH AN TOÀN CHO ỨNG DỤNG ỨNG DỤNG IOS VÀ ANDROID 105

Phụ lục 05. HƯỚNG DẪN THIẾT LẬP CHÍNH SÁCH BẢO MẬT HĐH WINDOWS SERVER 2012 128

Phụ lục 06. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT ĐỐI VỚI WEB SERVER 148

Phụ lục 07. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT ĐỐI VỚI WEB SERVER 154

Phụ lục 08. HƯỚNG DẪN THIẾT LẬP QUY TẮC CẤU HÌNH ATTT CHO HỆ QUẢN TRỊ CƠ CỞ DỮ LIỆU 162

Phụ lục 09. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HỆ THỐNG EMAIL SỬ DỤNG EXCHANGE 2016 VÀ MAIL GATEWAY FORTIMAIL 174

Phụ lục 10. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HỆ THỐNG ACTIVE DIRECTORY 191

Phụ lục 11. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HỆ THỐNG WEB SECURITY BLUECOAT 203

Phụ lục 12. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HỆ THỐNG KASPERSKY SECURITY CENTER 217

Phụ lục 13. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HỆ THỐNG VPN SỬ DỤNG FIREWALL PALOALTO 237

Phụ lục 14. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO THIẾT BỊ FIREWALL 246

Phụ lục 15. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO THIẾT BỊ THIẾT BỊ MẠNG CISCO VÀ JUNIPER 353

Phụ lục 01.
HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HĐH WINDOWS CỦA NGƯỜI DÙNG CUỐI

I. HƯỚNG DẪN THỰC HIỆN THỦ CÔNG TRÊN CÁC MÁY TÍNH

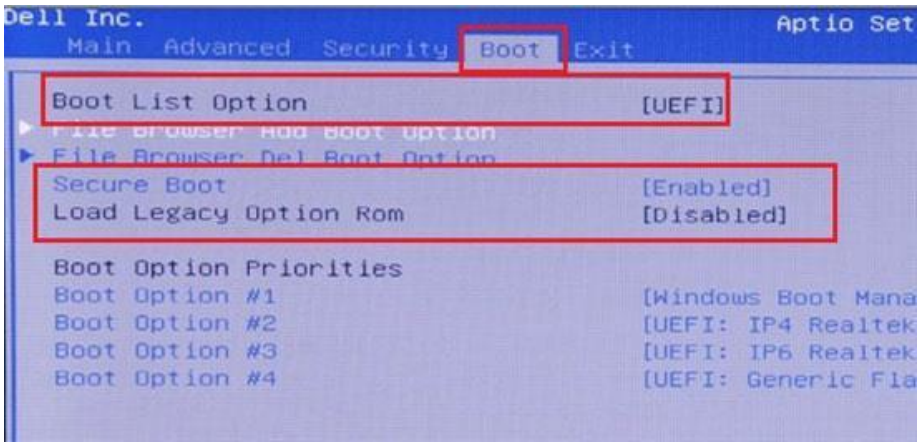
1. Cài đặt BIOS máy tính

Bước 1: Khởi động máy tính và truy cập truy cập vào BIOS theo mainboard:

- **Mainboard Abit** - Bấm phím **DEL** để vào BIOS Setup Utility.
- **Mainboard ASRock** - Bấm phím **F2** để vào BIOS Setup Utility.
- **Mainboard ASUS** - Bấm phím **DEL, Print** hoặc **F10** để vào BIOS Setup Utility.
- **Mainboard BFG** - Nhấn **DEL** để vào BIOS Setup Utility.
- **Mainboard FREESCALE** - Nhấn **DEL** để vào BIOS Setup Utility.
- **Mainboard DFI** - Nhấn **DEL** để vào BIOS Setup Utility.
- **Mainboard ECS Elitegroup** - Bấm phím **DEL** hoặc **F1** để vào BIOS Setup Utility.
- **Mainboard EVGA** - Bấm phím **Del** để vào BIOS Setup Utility.
- **Mainboard Foxconn** - Nhấn **Del** để vào BIOS Setup Utility.
- **Mainboard GIGABYTE** - Bấm phím **Del** để vào BIOS Setup Utility.
- **Mainboard Intel** - Bấm phím **F2** để vào BIOS Setup Utility.
- **Mainboard JetWay** - Bấm phím **DEL** để vào BIOS Setup Utility.
- **Mainboard Mach Speed** - Bấm phím **DEL** để vào BIOS Setup Utility.
- **Mainboard MSI (Micro-Star)** - Bấm phím **DEL** để vào BIOS Setup Utility.
- **Mainboard PCChips** - Bấm phím **DEL** hoặc **F1** để vào BIOS Setup Utility.
- **Mainboard SAPPHIRE** - Bấm phím **DEL** để vào BIOS Setup Utility.
- **Mainboard Shuttle** - Bấm phím **Del** hoặc **Ctrl + Alt + Esc** phím để vào tiện ích thiết lập BIOS.
- **Mainboard Soyo** - Bấm phím **DEL** để vào BIOS Setup Utility.
- **Mainboard Supermicro** - Bấm phím **DEL** để vào BIOS Setup Utility.
- **Mainboard TYAN** - Bấm phím **DEL** hoặc **F4** để vào BIOS Setup Utility.
- **Mainboard XFX** - Bấm phím **DEL** để vào BIOS Setup Utility.

Bước 2: Truy cập vào **BIOS** => tìm đến tab **BOOT** => tìm đến phần **Boot Option**:

- Boot List Option chọn là "**UEFI**"

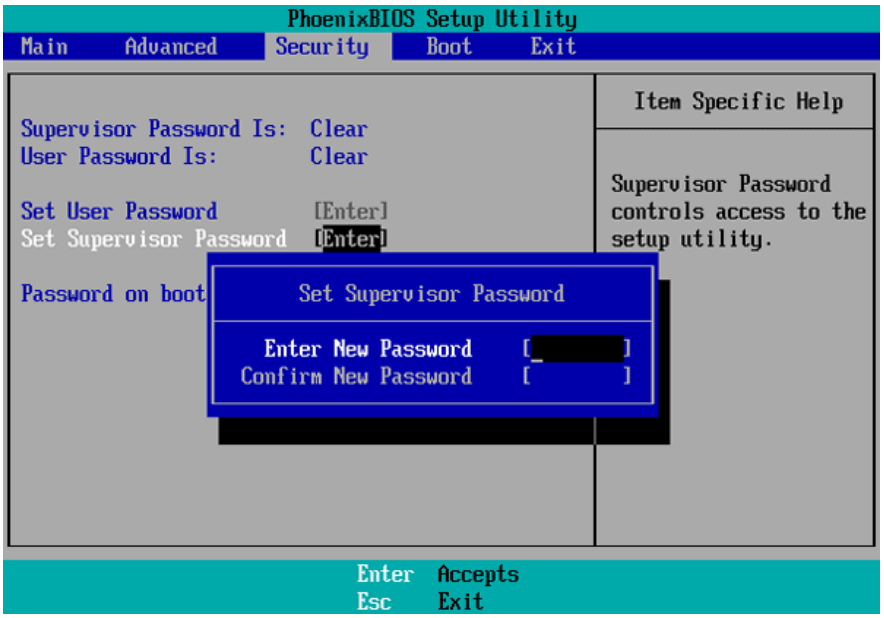


- Secure Boot: chọn "**Enable**"

- First Boot Device => Chọn "**Hard Disk**"

- Truy cập Power: Chọn **Wake-On LAN** => Chọn "**Disable**"

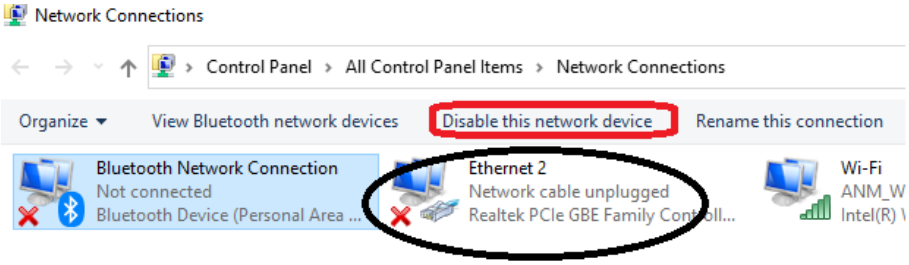
- Truy cập Security: Cài đặt mật khẩu BIOS (tùy chọn).



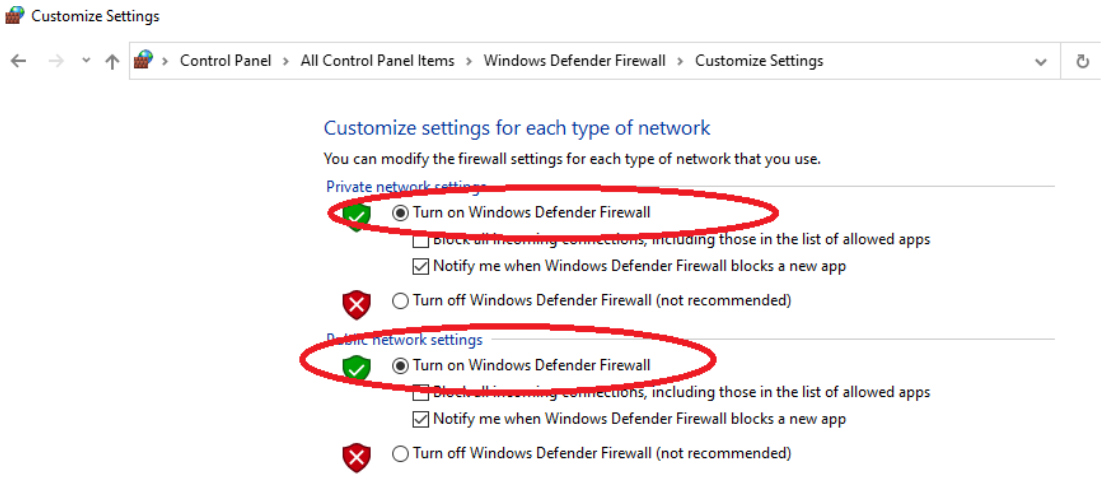
- Thiết lập lại tất cả các cấu hình BIOS trong trường hợp pin CMOS được thay thế, hoặc bị tháo ra.

2. Thiết lập cấu hình mạng trên hệ điều hành

- Disable các network interface không sử dụng: Mở **Control Panel** => **All Control Panel Items** => **Network Connections.**

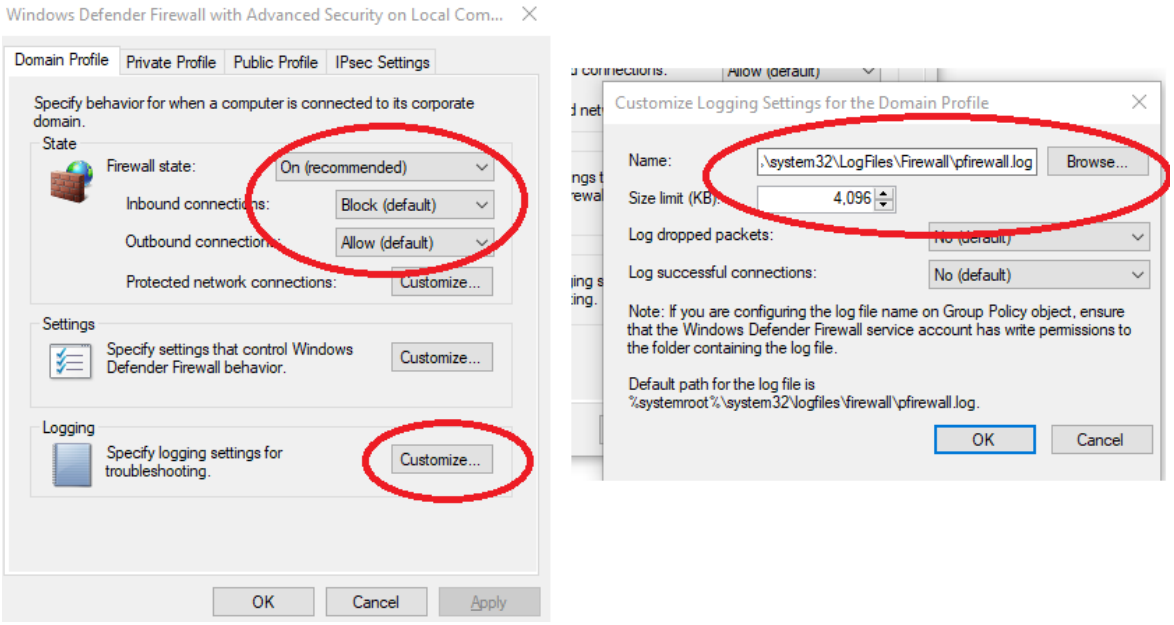


- Tường lửa của hệ điều hành hoặc của phần mềm antivirus phải luôn được bật. Cấu hình ghi log: Mở **Control Panel** => **All Control Panel Items** => **Windows Defender Firewall** => **Advanced settings** => **Customize Settings** => Chọn **Turn on Windows Defender Firewall.**

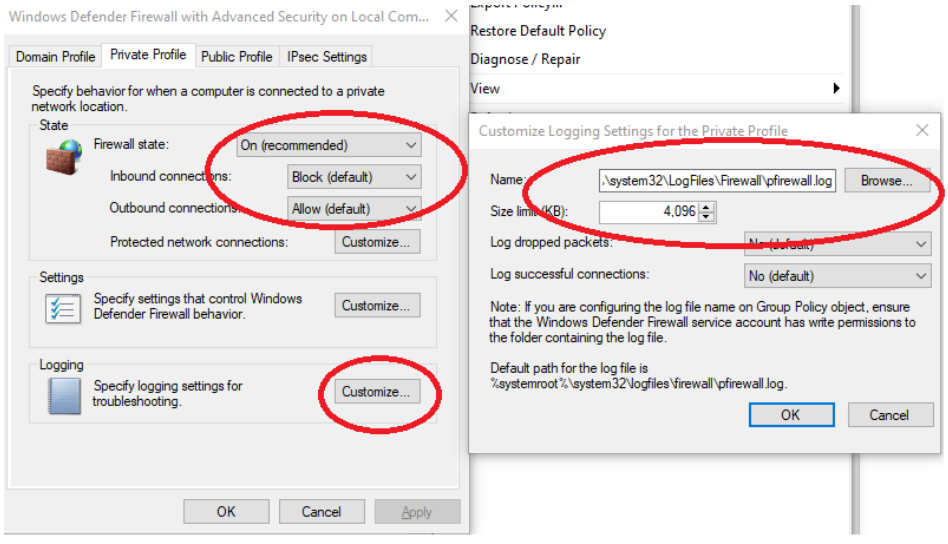


Chọn các Tab:

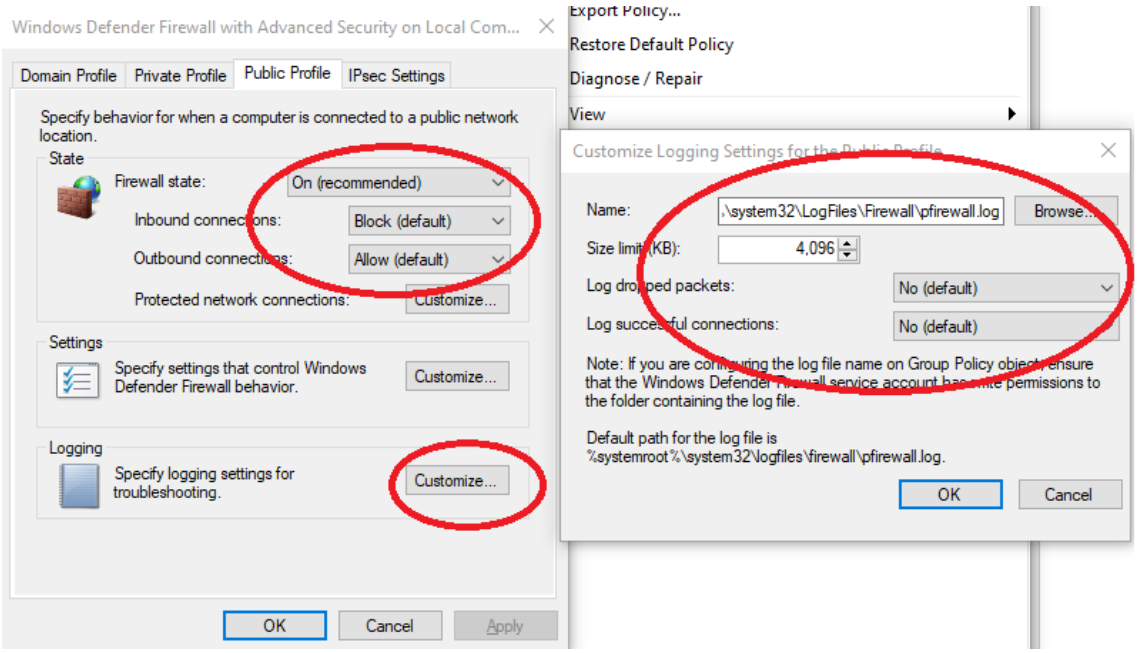
+ **Domain Profile**:



+ **Private Profile**:

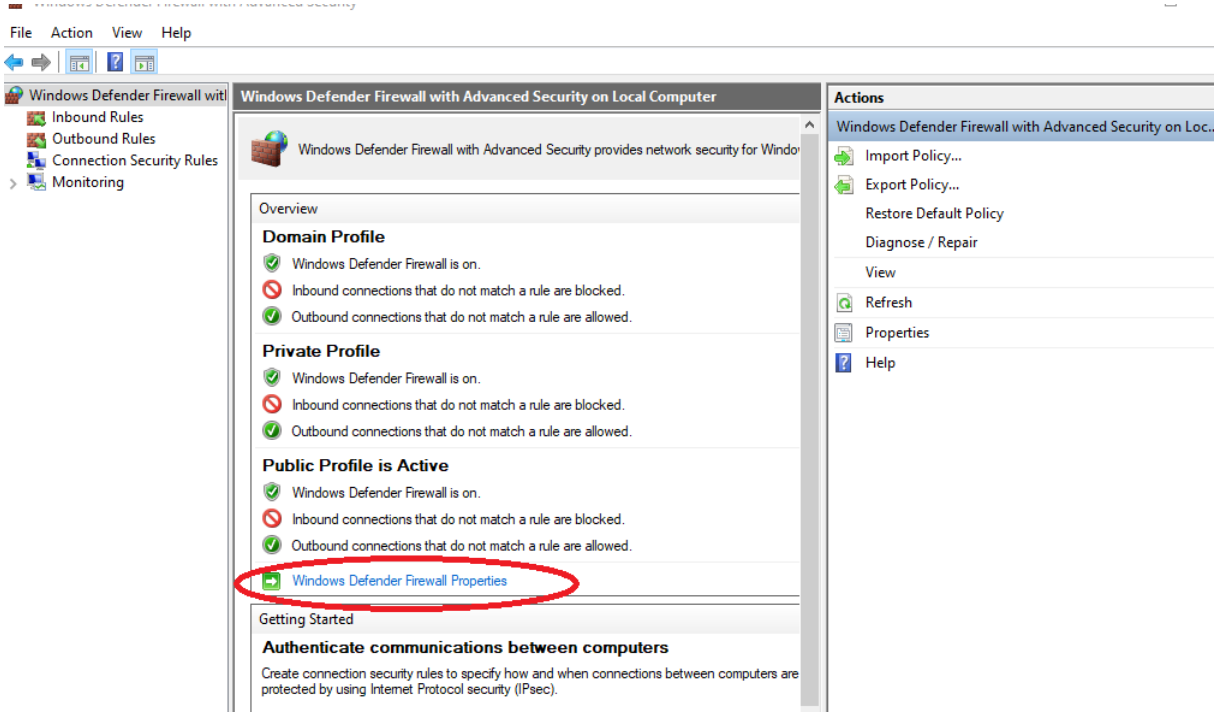


+ **Public Profile:**

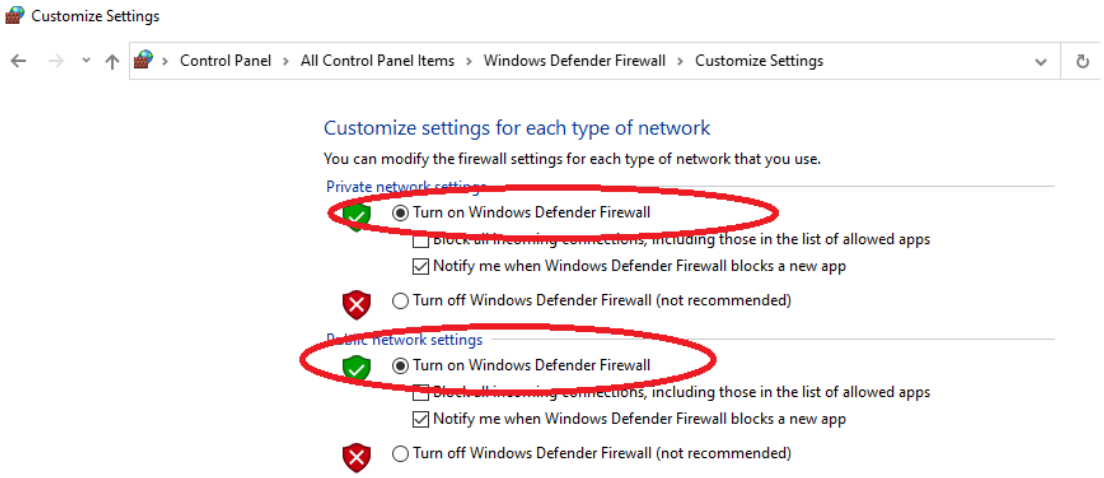


- Thiết lập chính sách tường lửa chiều vào (Inbound) và chiều ra (Outbound).

+ Chọn **Windows Defender Firewall Properties**

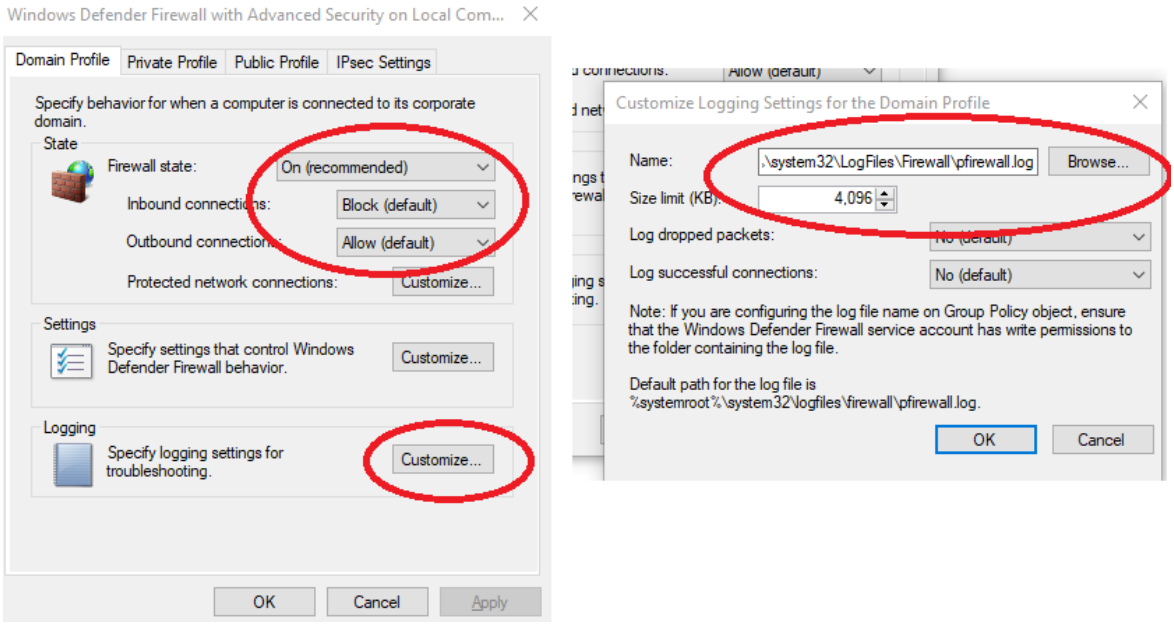


+ Mở **Control Panel** => **All Control Panel Items** => **Windows Defender Firewall** => **Advanced settings** => **Customize Settings** => Chọn **Turn on Windows Defender Firewall**

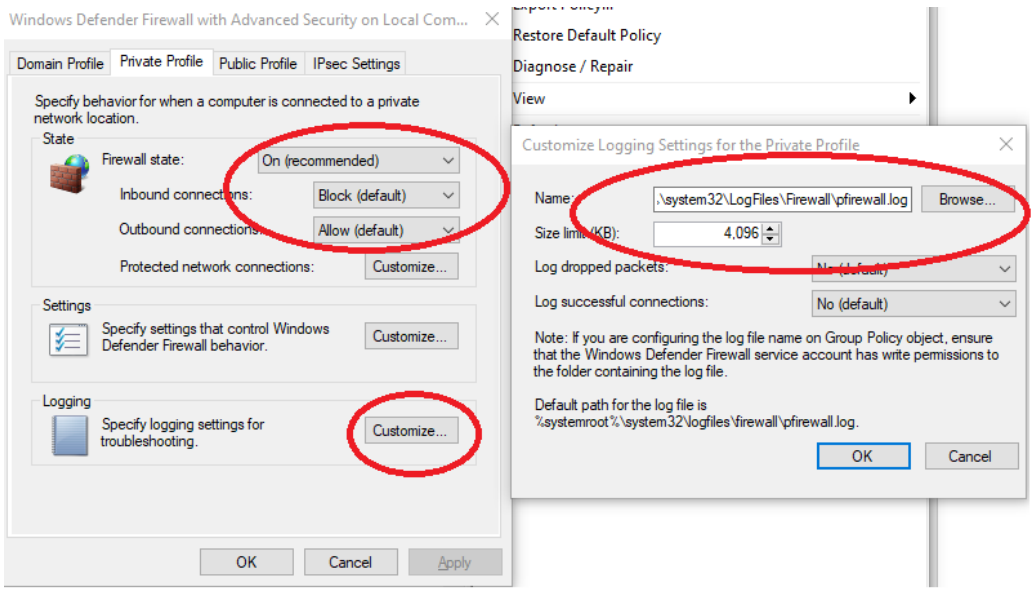


Chọn các Tab:

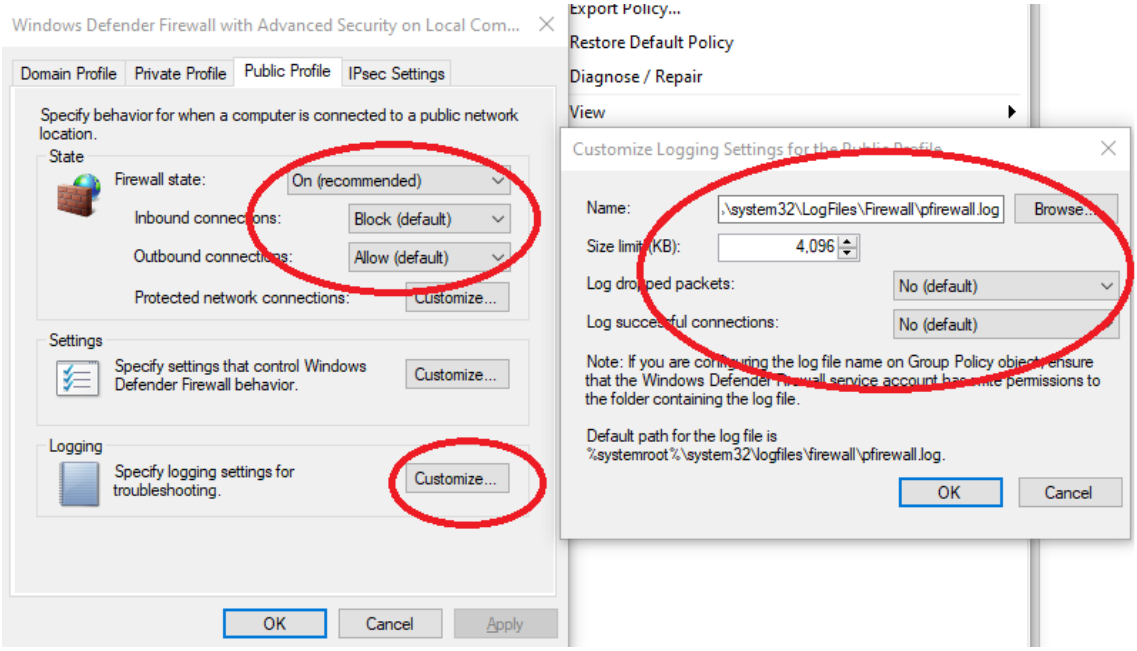
+ **Domain Profile:**



+ **Private Profile:**

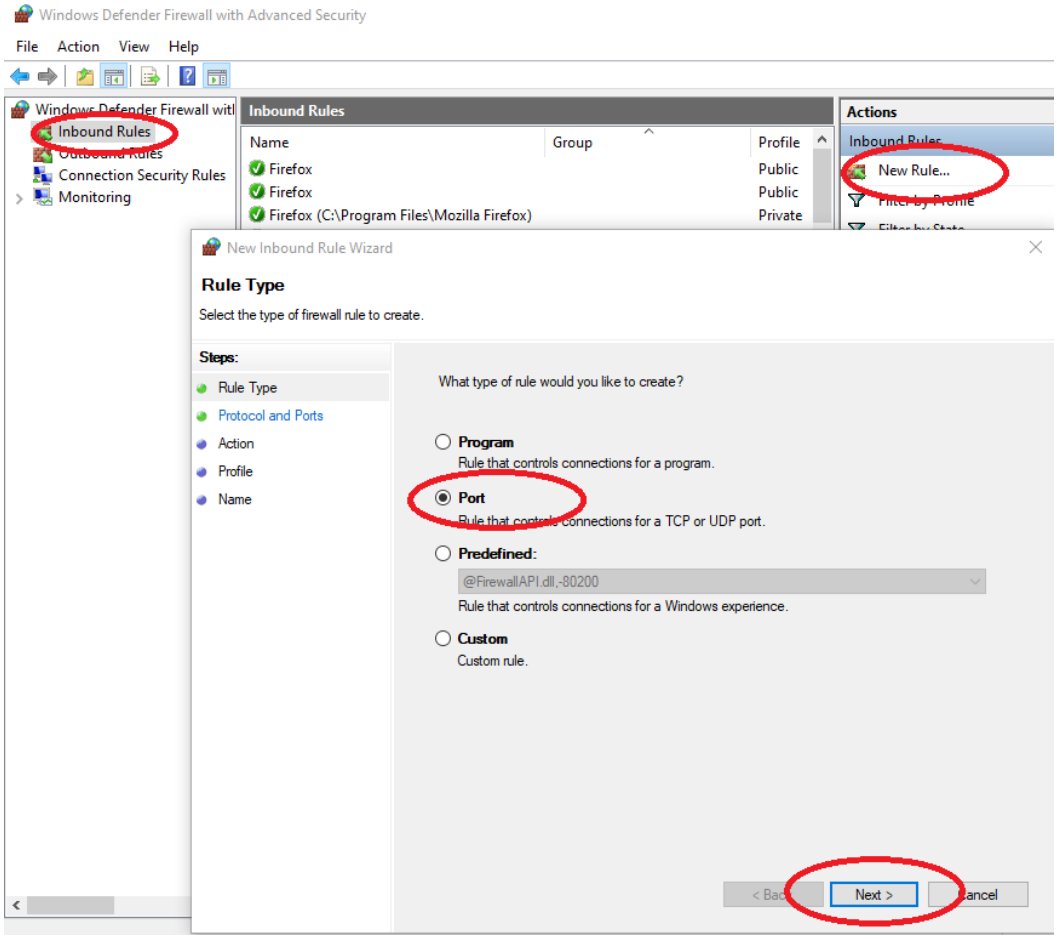


+ **Public Profile:**

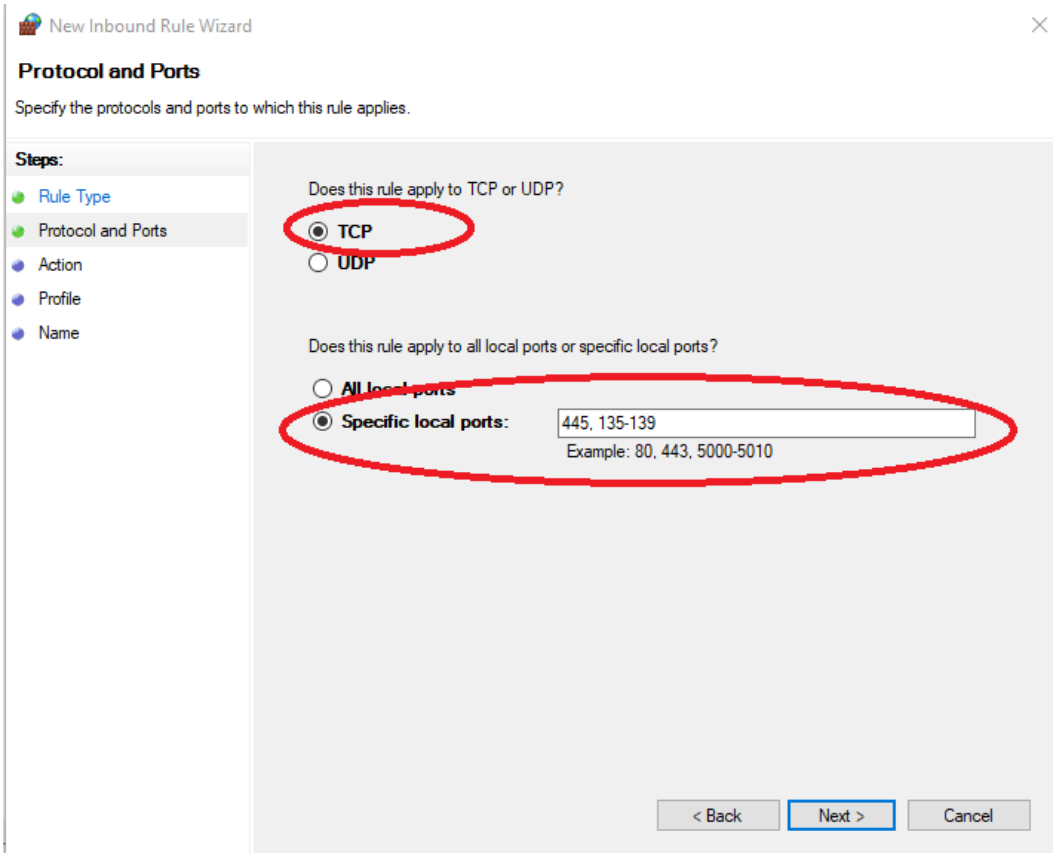


- Cấu hình chặn kết nối giữa các máy người dùng với nhau theo các cổng sau: 135->139 (NetBIOS), 445 (windows shared)

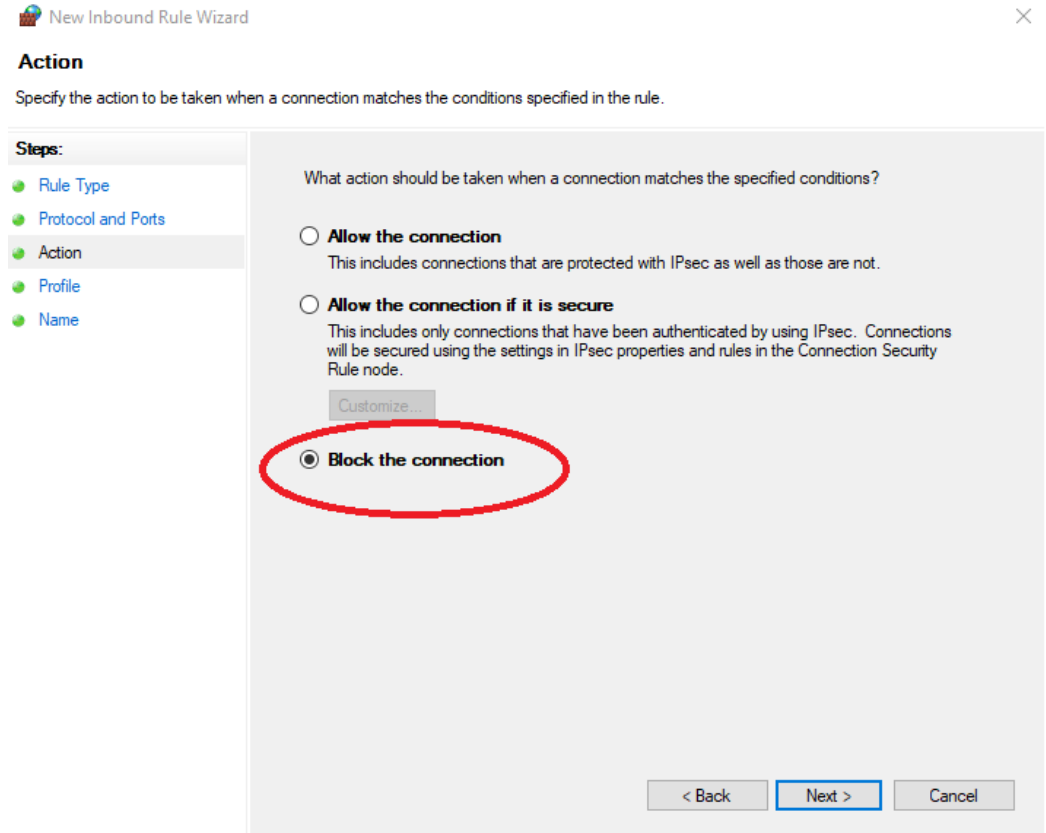
+ Chọn **Inbound Rules** => **New Rule...** => **Port** => **Next**



+ Thiết lập chặn các cổng => Chọn **Next**



+ Chọn **Block the connection** => Chọn **Next** => **Next**



+ Đặt tên Rule và chọn **Finish**

+ Kéo thả Rule lên vị trí/thứ tự đầu tiên.

- Sử dụng Proxy của đơn vị để truy cập Internet, không truy cập Internet trực tiếp: Thực hiện theo thông báo/hướng dẫn của quản trị hệ thống/ATTT của đơn vị.

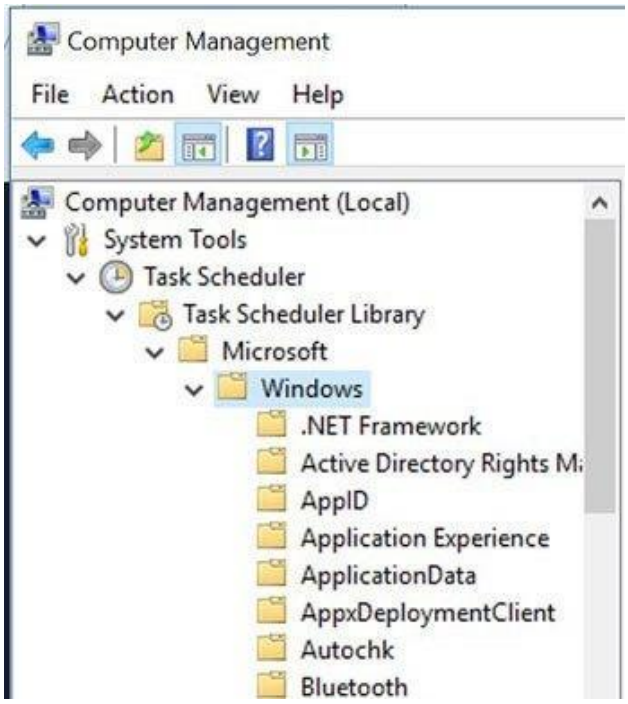
- Sử dụng cấu hình DNS của tập đoàn: Thực hiện theo thông báo/hướng dẫn của quản trị hệ thống/ATTT của đơn vị.

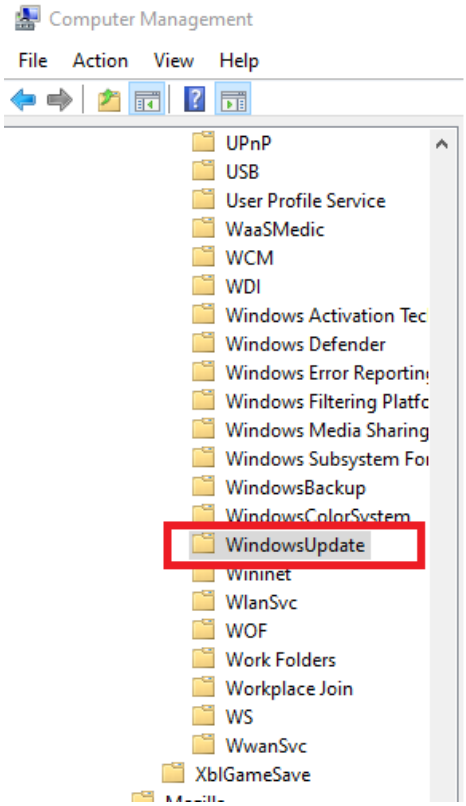
3. Cài đặt, cấu hình hệ điều hành

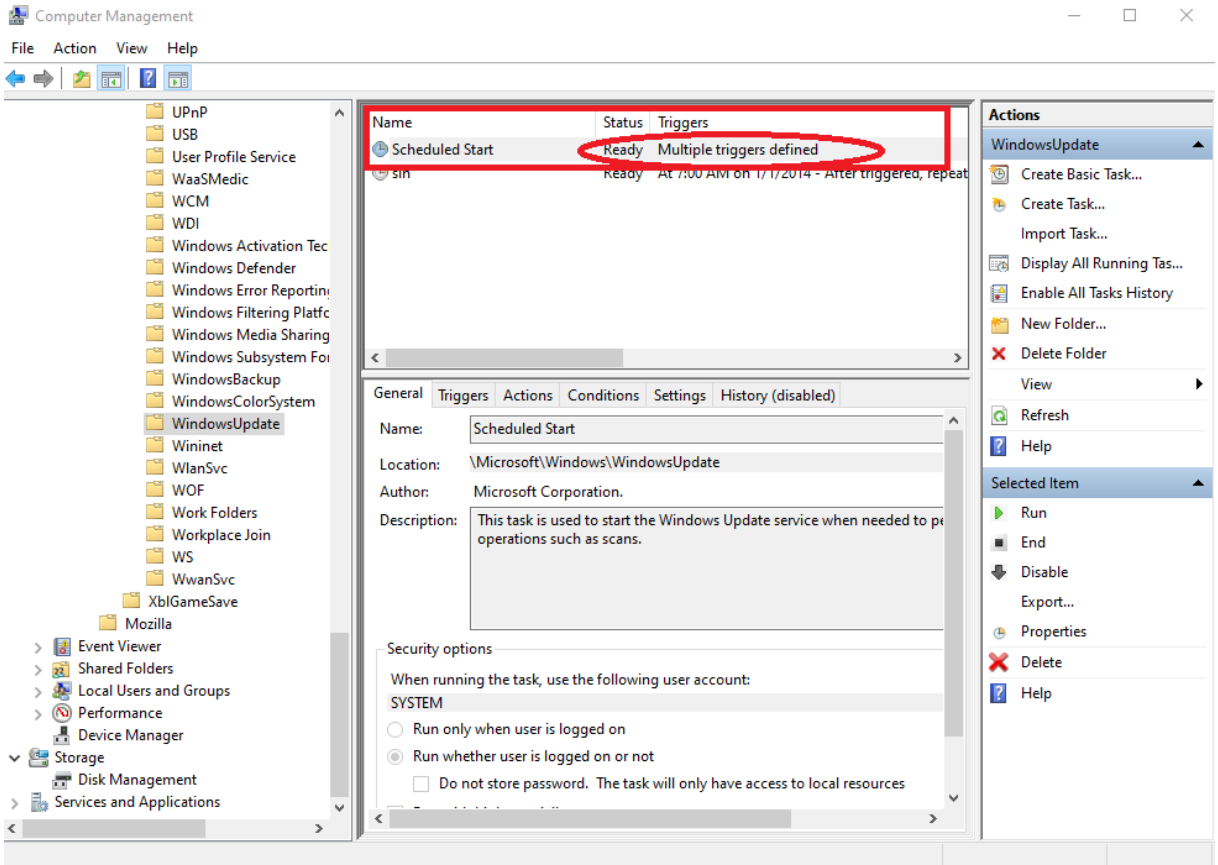
- Cài đặt phiên bản hệ điều hành trong vòng đời sản phẩm Windows do Microsoft cung cấp tại https://support.microsoft.com/en-us/lifecycle/search/1163.

- Sử dụng license hợp lệ của đơn vị để active.

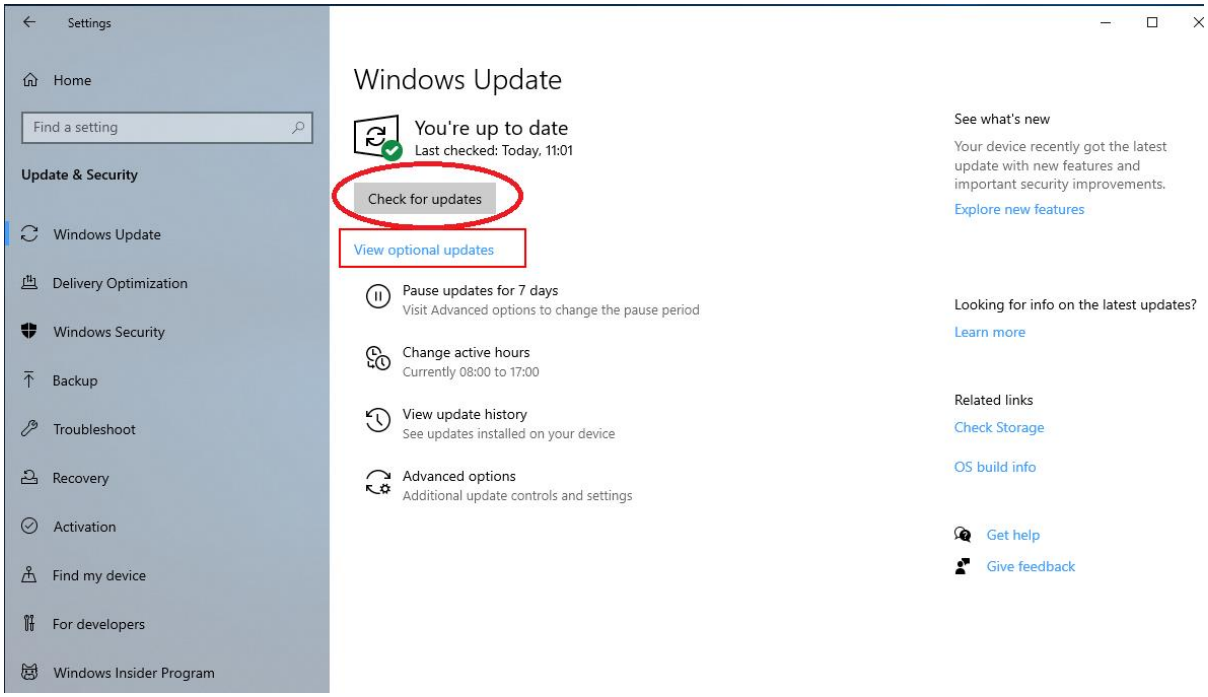
- Cấu hình update: Chọn **My Computer** => **Manager** => **System Tools** => **Task Scheduler** => **Task Scheduler Library** => **Microsoft** => **Windows** => **Windows Update**







Chọn **Start** => **Settings** => **Update & Security** => **Windows Update**



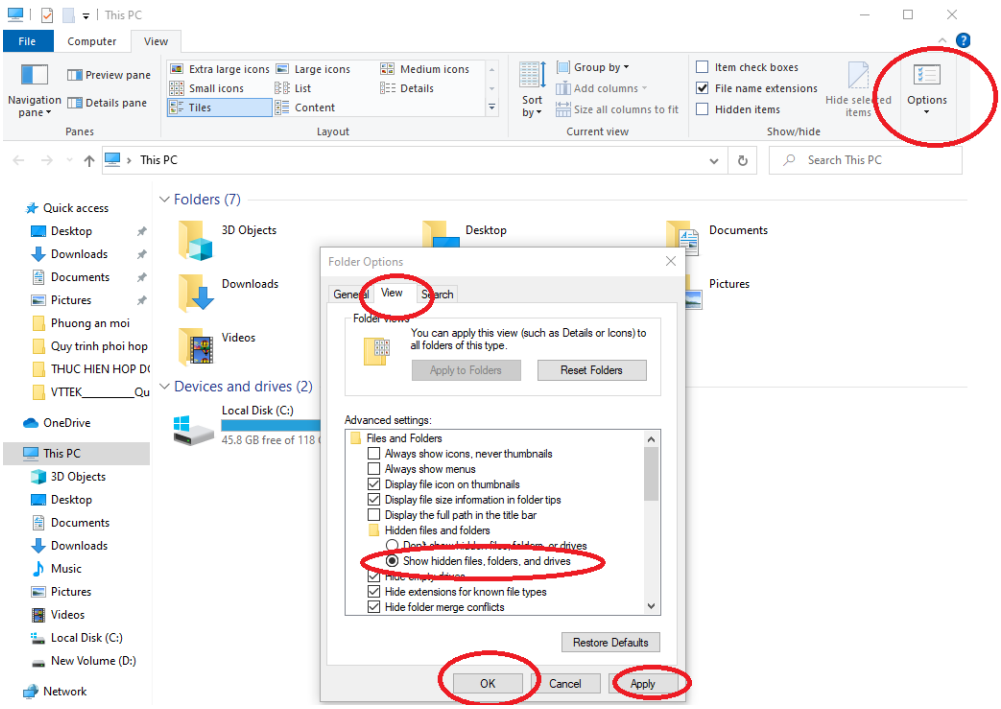
<u>Note:</u> Đối với các đơn vị triển khai hệ thống AD: Triển khai hệ thống WSUS để cập nhật bản vá tập trung cho toàn bộ máy chủ/máy trạm.

- Yêu cầu thiết lập ghi log hệ thống: Mặc định đã có.
- Tắt chia sẻ mặc định, không cho phép người dùng chia sẻ file trên máy tính

+ Thực hiện tập trung bằng Group Policy trên AD.

+ Đối với máy tính người dùng: thực hiện vào Run => CMD => gõ ”net share” để kiểm tra các thư mục đang sharing => Thực hiện Disable share.

- Hiển thị đầy đủ định dạng tập tin (file extension) trên máy người dùng



4. Chính sách sử dụng phần mềm

- Không sử dụng các phần mềm chat client (ví dụ: skype, google talk, msn chat hoặc các phần mềm tương đương):

Chi tiết thực hiện tại mục 11 Phần 2.

- Không sử dụng các phần mềm bên ngoài cho phép remote, điều khiển máy tính từ xa (ví dụ: teamviewer, logmein, vnc, radmin, x-manager hoặc các phần mềm tương đương):

Chi tiết thực hiện tại mục 11 Phần 2.

- Không sử dụng các phần mềm vượt tường lửa, proxy như các phần mềm proxy, vpn, tunnel (ví dụ: hostspot shield, ultrasurf hoặc các phần mềm tương đương):

Chi tiết thực hiện tại mục 8 Phần 2

- Cài đặt phần mềm diệt virus và phần mềm giám sát bất thường:

Thực hiện theo quy định, chính sách hiện hành.

- Đối với phần mềm diệt virus:

Cấu hình theo quy định, chính sách hiện hành.

5. Thiết lập chính sách tài khoản, chính sách quản trị

- Máy tính phải được join domain

Join máy tính vào domain theo hướng dẫn của bộ phận quản trị hệ thống/ATTT.

- Người dùng phải dùng tài khoản domain để sử dụng máy tính

Chi tiết thực hiện tại mục 8 Phần 2. Với các đơn vị không triển khai hệ thống domain tập trung cần có sự phê duyệt của lãnh đạo đơn vị.

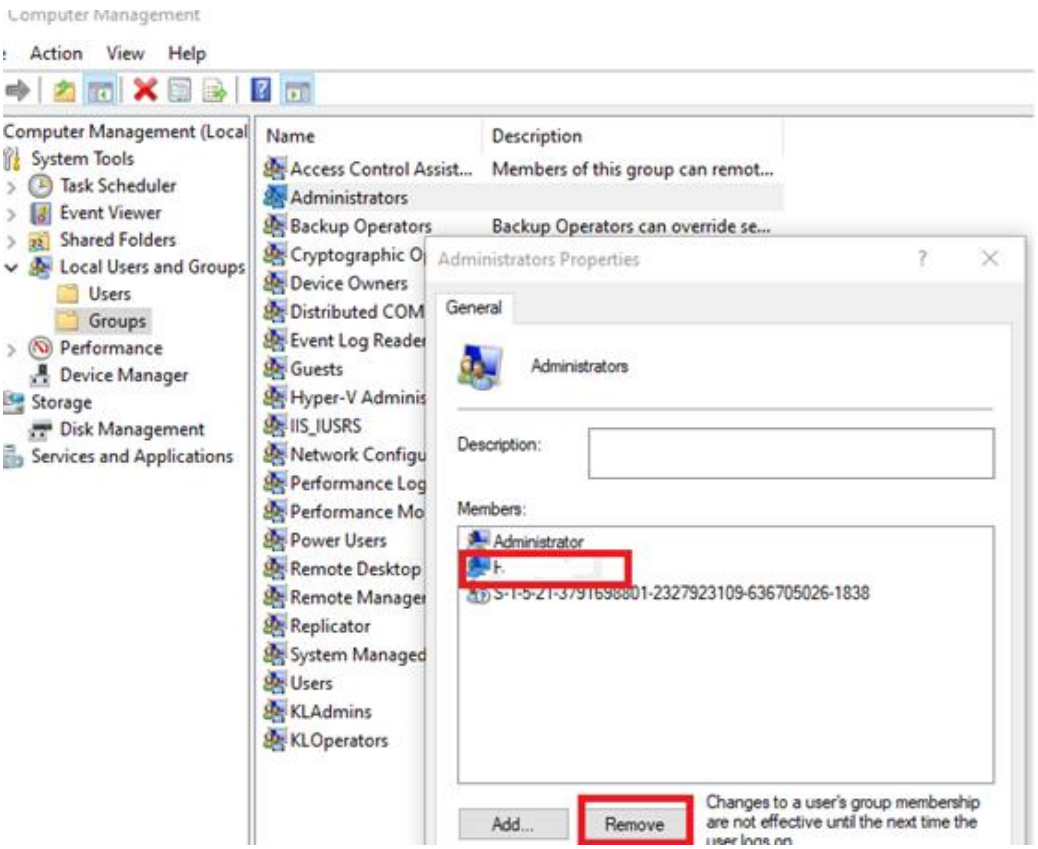
- Tên tài khoản chuẩn hóa.

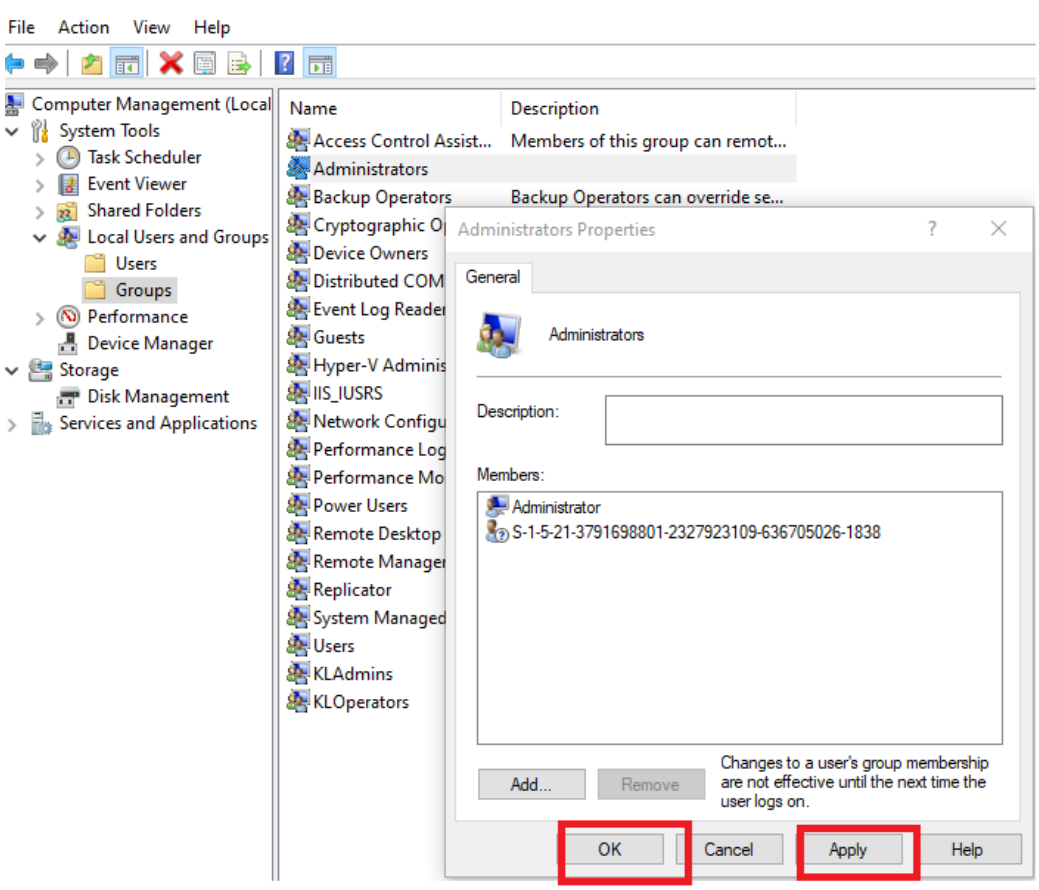
Khuyến nghị tên tài khoản được chuẩn hóa chung theo quy định tổ chức.

- Tên máy tính bao gồm tên theo tài khoản email người dùng và tên viết tắt của đơn vị

Khuyến nghị tên máy tính được chuẩn hóa chung theo quy định tổ chức

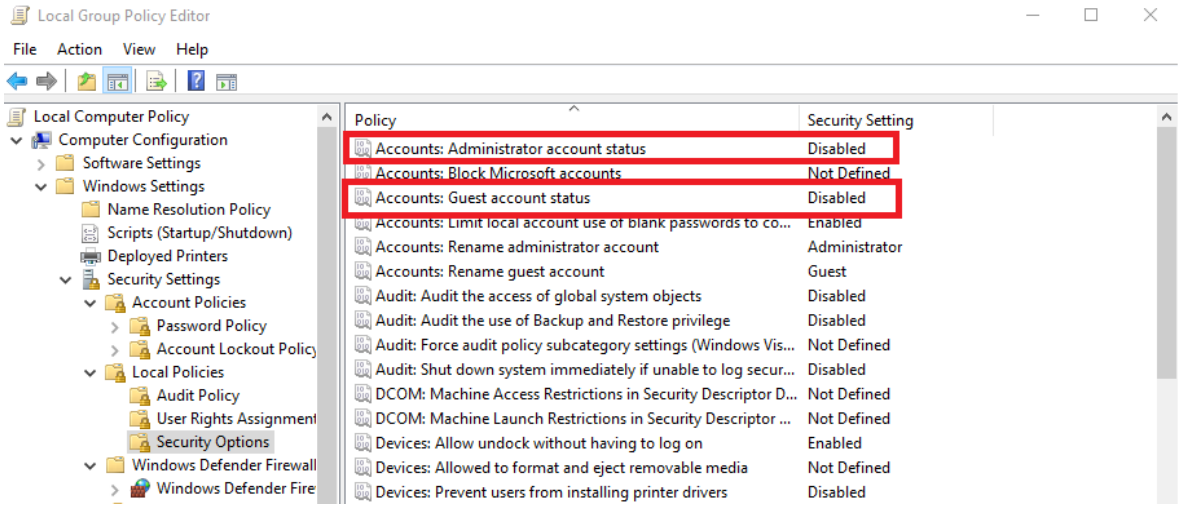
- Với các máy join domain, tài khoản người dùng không được có quyền administrator trên máy tính





- Xóa bỏ hoặc vô hiệu hóa tài khoản thừa, không sử dụng.

Loại bỏ tài khoản Guest, tắt và thu hồi tài khoản Administrator Local trên các máy tính join domain



- Giới hạn máy đăng nhập của người dùng với các máy join domain. Mỗi tài khoản người dùng chỉ được đăng nhập vào các máy tính được cho phép:

Chi tiết thực hiện tại mục 15 Phần 2.

- Cấu hình đồng bộ thời gian trên máy tính về server NTP tập trung hoặc thông qua server AD

Chi tiết thực hiện tại mục 2 Phần 2.

6. Chính sách sử dụng dữ liệu

- Tắt tính năng tự động chạy khi kết nối tới các thiết bị lưu trữ gắn ngoài, CD,..

Thực hiện thủ công trên máy không Join domain: Run => gpedit.msc => Computer Configuration => Administrative Template => Window Components => AutoPlay Policies => Thiết lập Turn off Autoplay giá trị Enabled -> OK

- Không cho phép máy tính người dùng sử dụng các thiết bị lưu trữ, đọc ghi dữ liệu (USB, Ổ cứng di động, ổ đĩa CD, DVD, ...)

Thực hiện trên Group Policy trên Domain.

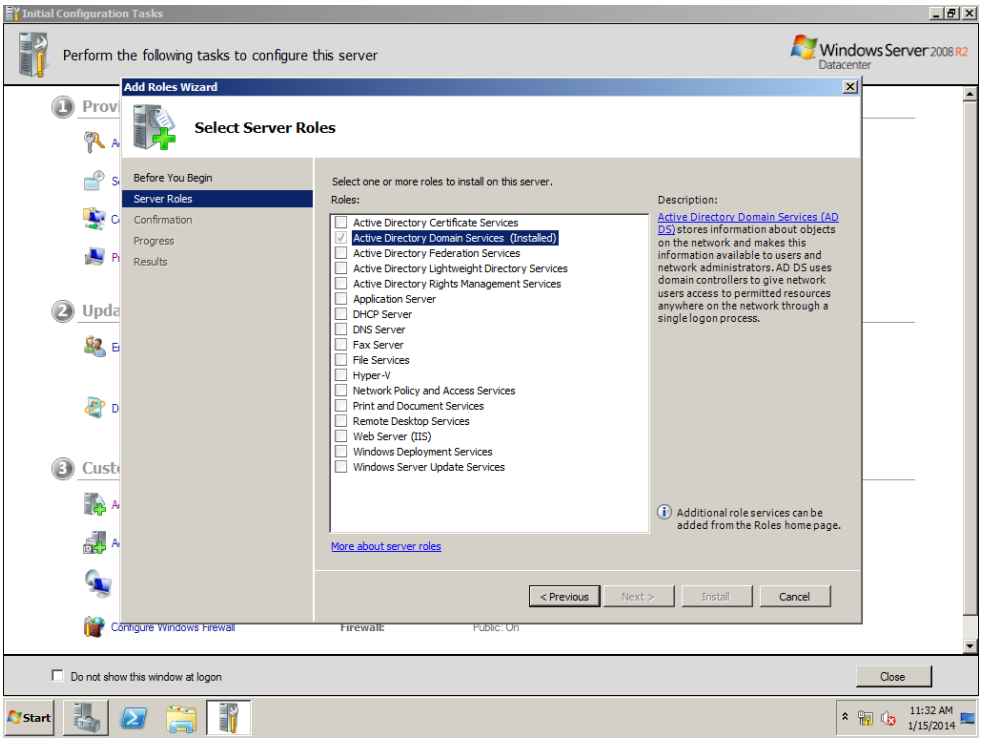
- Các dữ liệu mật, tài liệu quan trọng cần được lưu trữ trong thư mục, phân vùng có mã hóa hoặc được bảo vệ bởi phần mềm mã hóa (khuyến nghị).

Sử dụng các phần mềm mã hóa của đơn vị nếu có để mã hóa các dữ liệu mật, tài liệu quan trọng theo quy định nội bộ của đơn vị.

II. HƯỚNG DẪN THIẾT LẬP CHÍNH SÁCH ATTT TẬP TRUNG TRÊN DOMAIN CONTROLLER

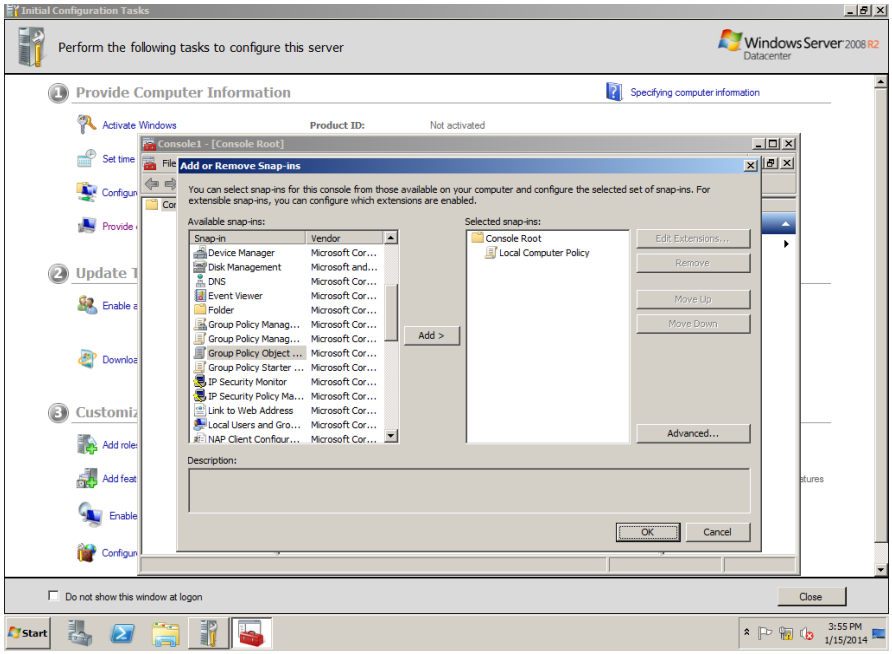
1. Lựa chọn role ”Active Directory Domain Services”

- Khi cài đặt chức năng AD DC, chỉ chọn ”Active Directory Domain Services” trong phần Add Roles Wizard



2. Đồng bộ thời gian với máy chủ NTP

- Start -> ”mmc” -> File -> Add/Remove Snap-In -> ”Group Policy Object Editor” -> Add -> Finish -> OK



- Chọn đến phần Local Computer Policy\Computer Configuration\Administrative Templates\System\Windows Time Service\Time Providers:

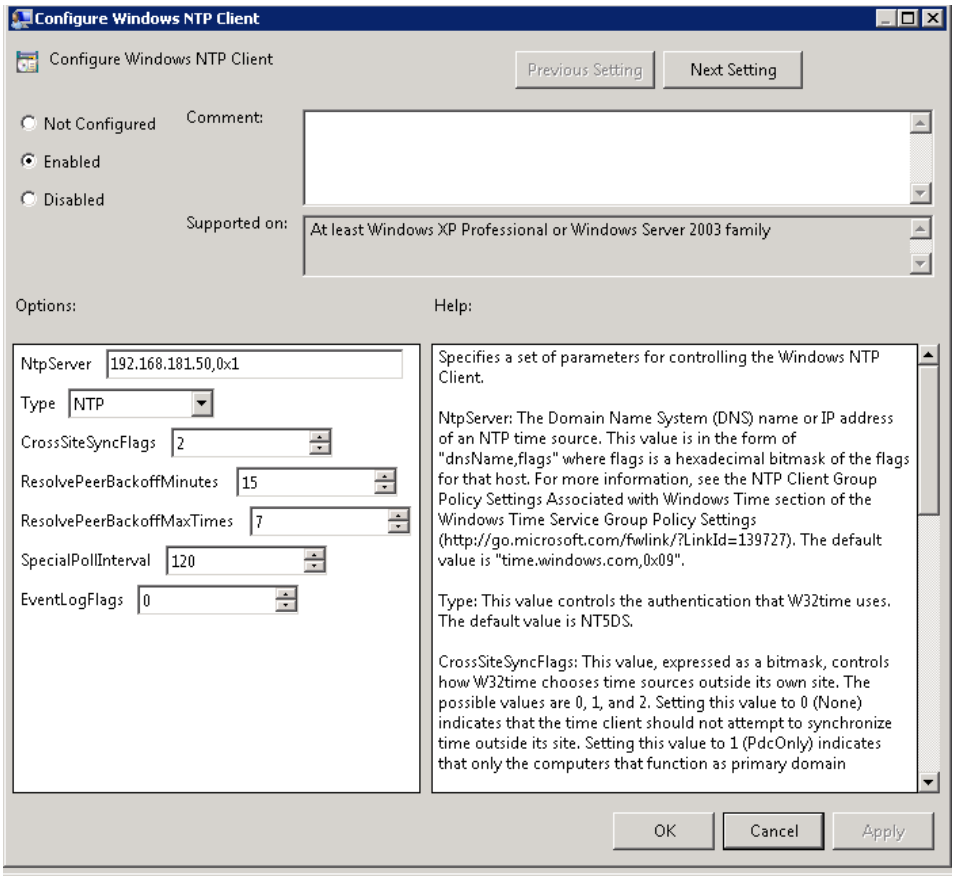
+ Enable Windows NTP Client -> Chọn Enabled

+ Enable Windows NTP Server-> Chọn Enabled

+ Configure Windows NTP Client -> Chọn Enabled.

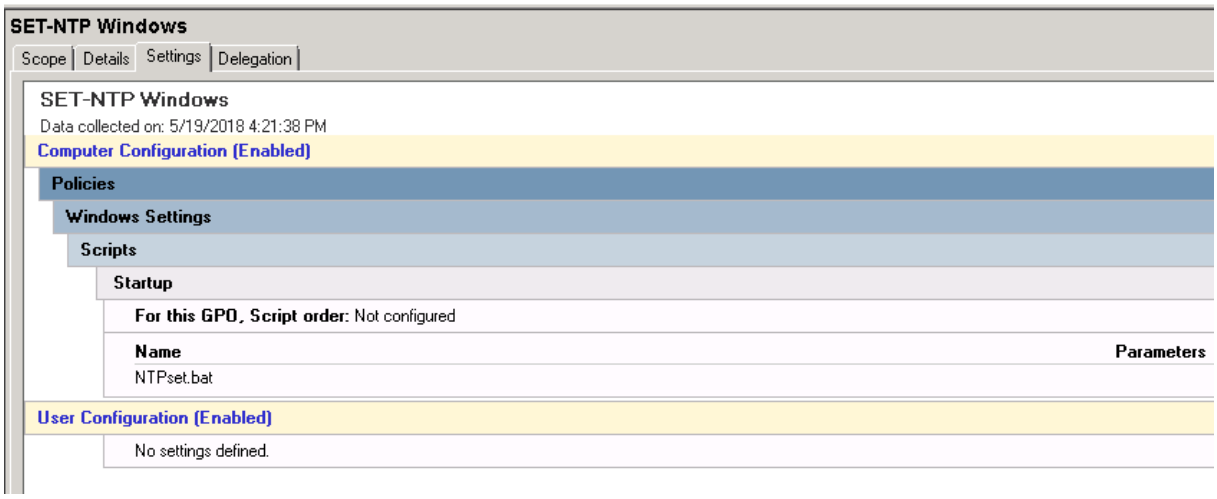
● Đặt "NTP Server" với giá trị là IP của server NTP. Tham số 0x1 ở sau địa chỉ IP chỉ định đồng bộ hóa với mỗi chu kỳ 'SpecialPollInterval'.

● Đặt "Type" là "NTP" -> thiết lập "SpecialPollInterval" giá trị "120" -> Ok



<u>Ghi chú:</u> Có thể tạo file .bat với nội dung sau và add cho máy tính (Computer Configuration) người dùng chạy khi khởi động để đồng bộ thời gian

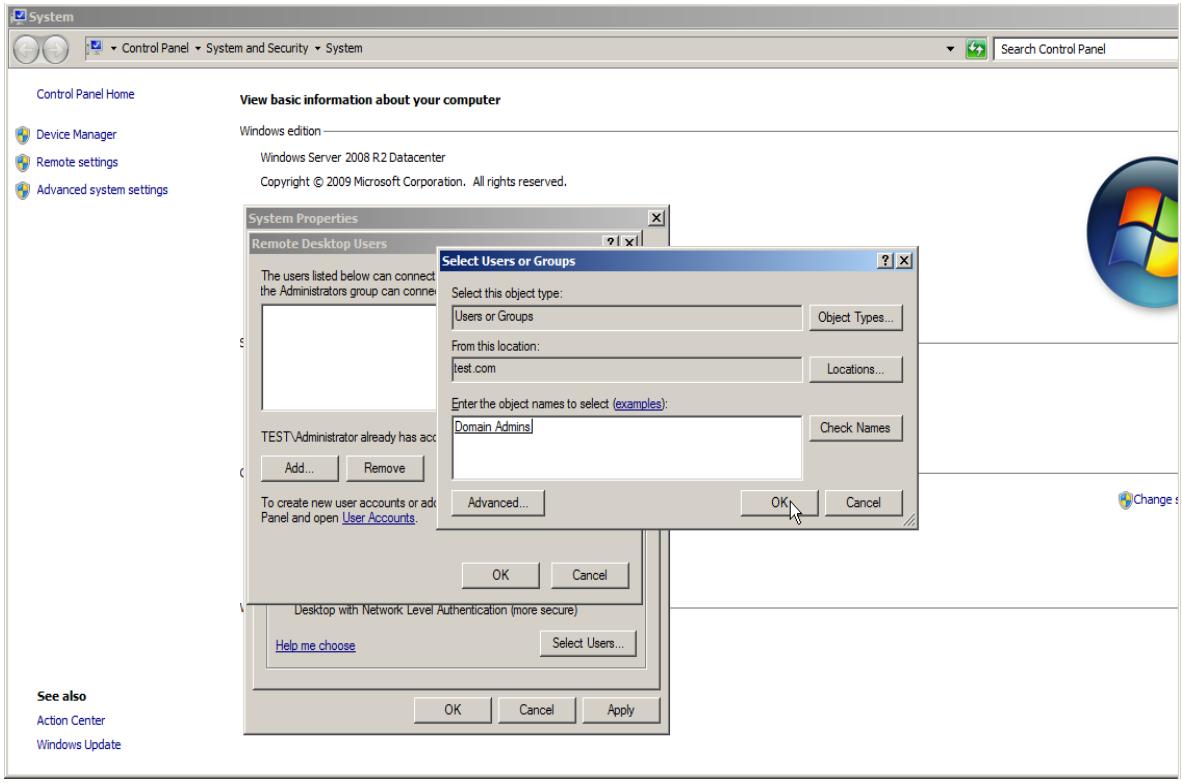
- w32tm /config /syncfromflags:domhier /update
- net stop w32time
- net start w32time



3. Giới hạn tài khoản quản trị dịch vụ AD

3.1. Giới hạn tài khoản remote desktop

- Start -> click chuột phải vào Computer -> Properties -> Remote Settings -> Allow connection from computers running any version of Remote Desktop -> Select Users -> Add -> nhập các user/group có thẩm quyền được remote desktop -> Ok



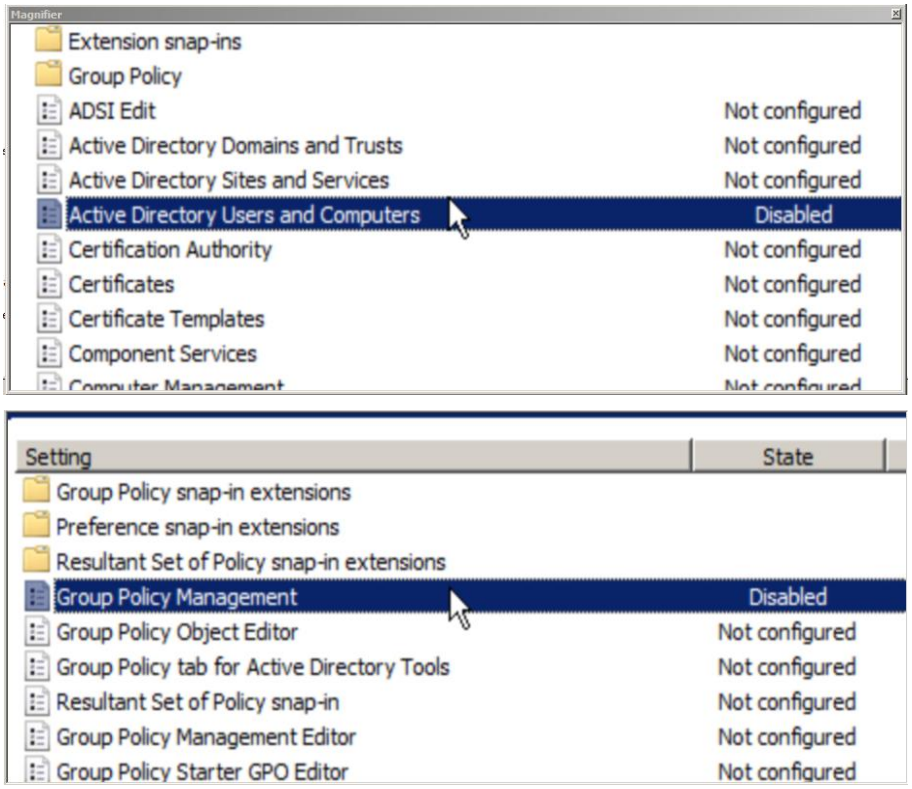
3.2. Giới hạn tài khoản quản trị dịch vụ AD từ ra sử dụng remote tool Remote Server Administration Tools từ những tài khoản có thẩm quyền (những tài khoản được ủy quyền quản trị)

- Start -> gõ ”Group Policy Management -> tạo 01 GPO tên là “Disable Remote tools” và 01 GPO tên là “Enable Remote tools”

- Click chuột phải vào GPO “Disable Remote tools” -> Edit -> User Configuration/ Policies/ Administrative Templates/ Windows Components/ Microsoft Management Console/ Restricted/Permitted snaps-in:

+ Chỉnh mục “Active Directory Users and Groups” thành “Disabled”

+ Chỉnh mục “Group Policy Management” thành “Disabled”

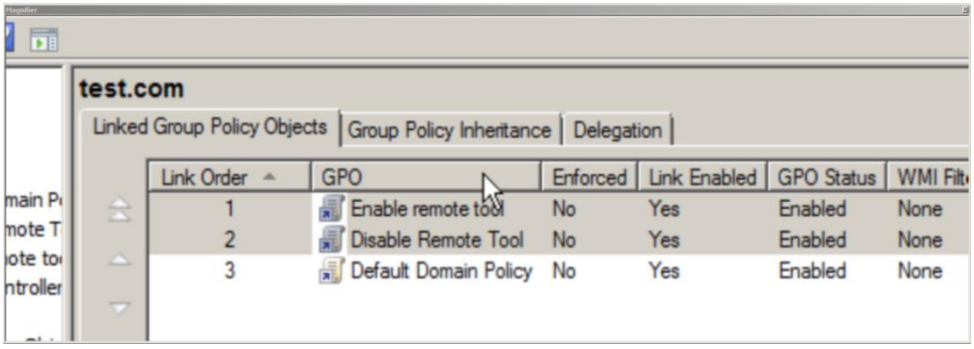


- Click chuột phải vào GPO “Enable Remote tools” -> Edit -> User Configuration/ Policies/ Administrative Templates/ Windows Components/ Microsoft Management Console/ Restricted/Permitted snaps-in:

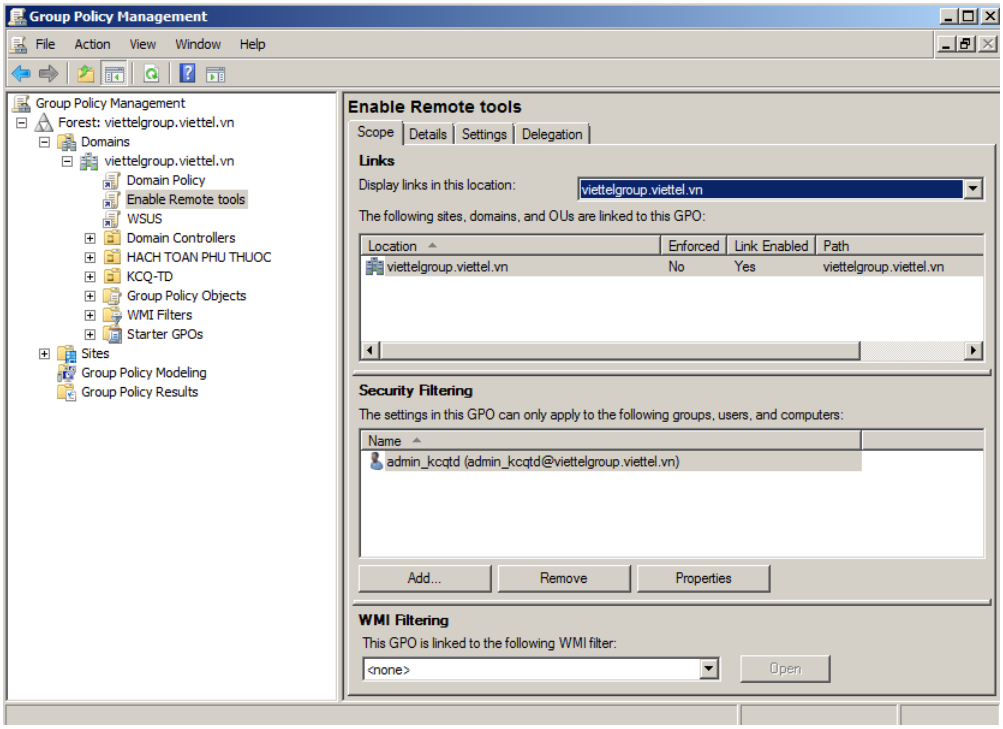
+ Chỉnh mục “Active Directory Users and Groups” thành “Enabled”

+ Chỉnh mục “Group Policy Management” thành “Enabled”

- Trong Group Policy Management, ấn vào tên domain -> Trong tab Linked Group Policy Objects, đặt lại link order để cho GPO “Enable Remote tools” đứng trước GPO “Disable Remote tools”



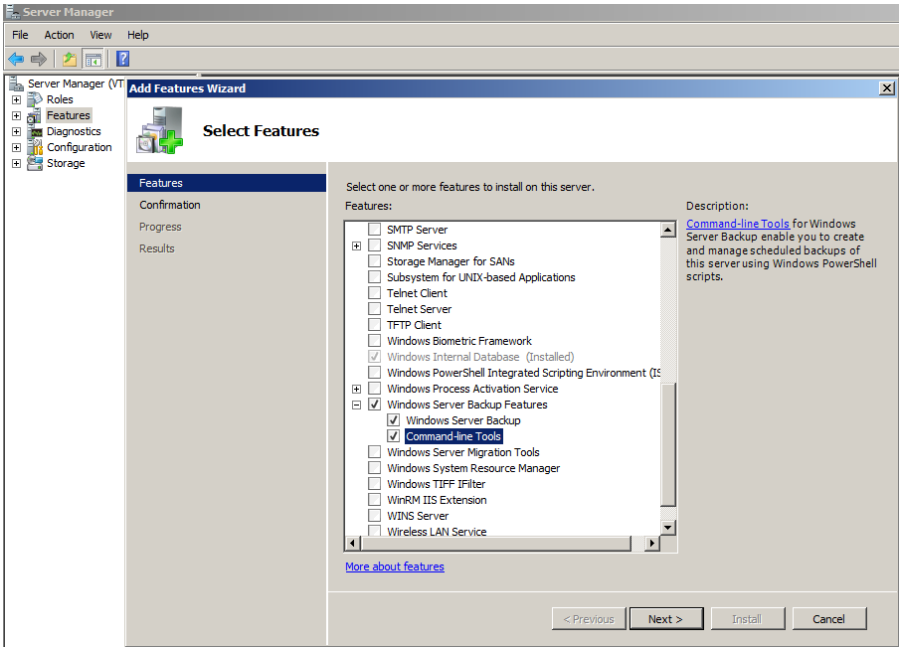
- Chọn GPO “Enable Remote tools” -> trong phần Security Filtering -> chọn Authenticated Users -> chọn Remove -> Chọn Add -> điền tên user/group quản trị bằng tool RSAT -> OK



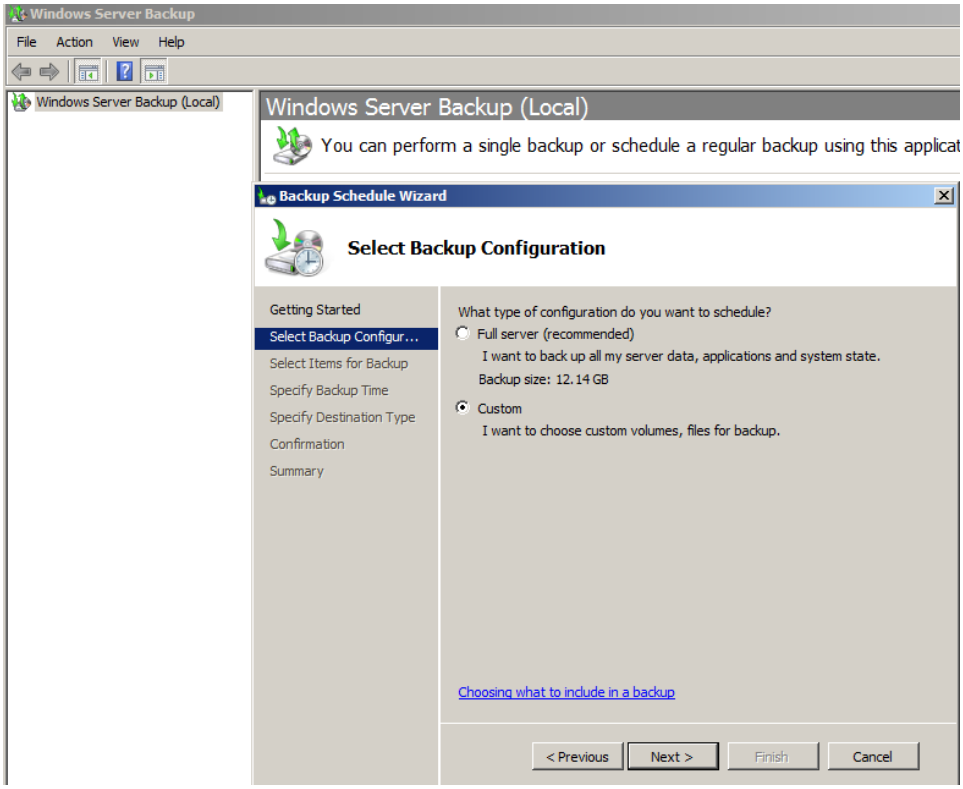
4. Sao lưu hệ thống định kỳ

Thực hiện sao lưu systemstate trên máy chủ Domain Controller định kỳ 01 lần/01 ngày và trước mỗi lần tác động. Thời gian lưu tối thiểu 01 tháng và ít nhất 02 bản sao lưu gần nhất, các bản sao lưu được đặt ở 02 nơi khác nhau.

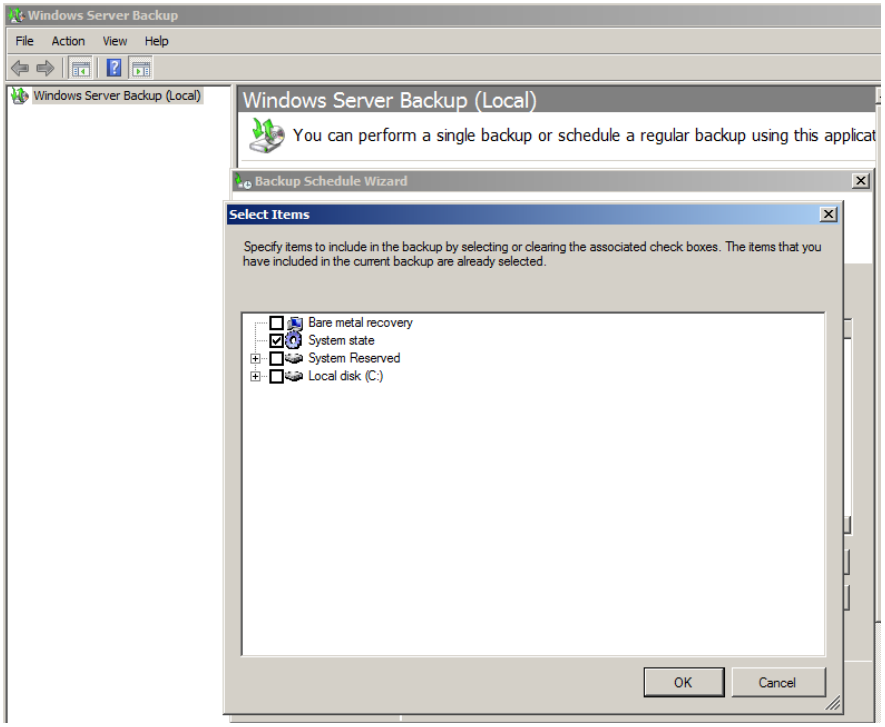
- Start -> Server Manager -> Features -> Add Features -> Chọn Windows Server Backup và Command-line Tools -> next -> Install -> Close để kết thúc.



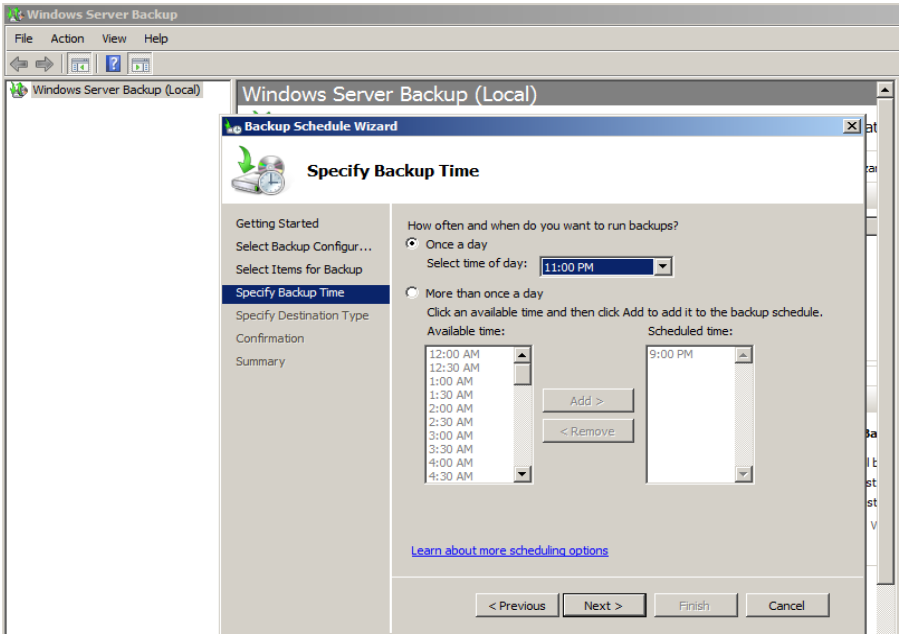
- Start -> Administrative -> Tools -> Click chuột phải vào Windows Server Backup -> Backup Schedule -> Next -> Chọn Custom -> Next



Chọn Add Items -> Chọn các phân vùng cần backup (ở đây chọn System state để backup Domain Controller) -> Ok



Click Next -> Chọn thời gian Backup định kỳ (11h đêm hàng ngày) -> Click Next



Click Next -> Chọn nơi lưu trữ (ổ cứng, ổ đĩa, thư mục chia sẻ qua mạng) -> Next -> Chọn nơi lưu trữ Backup -> Next -> Xác nhận thông tin -> Ok

5. Chính sách về tài khoản và mật khẩu

5.1. Đặt tên tài khoản (account) và tên máy tính (computer name) người dùng

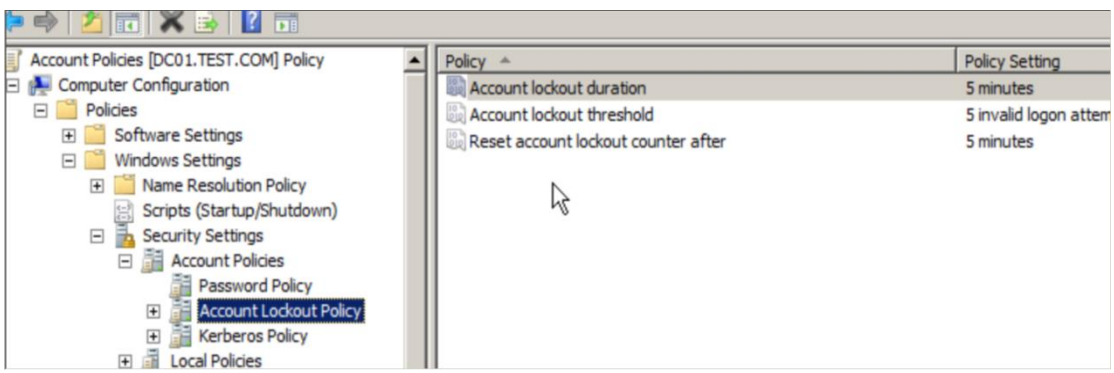
Tên tài khoản và tên máy tính người dùng: là tên đăng nhập (ID) trong địa chỉ email @XYZ.com.vn của người dùng. Ví dụ: **ANV** là tên tài khoản và tên máy tính của đồng chí có địa chỉ email ANV@XYZ.com.vn

Lưu ý: độ dài tên máy tính tối đa 15 ký tự.

5.2. Chính sách về tài khoản

- Click chuột phải vào GPO "Domain Policy" -> Edit -> Mở tới Computer Configuration/ Policies/ Windows Settings/ Security Settings/ Account Policies/ Account Lockout Policy -> thiết lập các giá trị:

+ Đặt Account lockout threshold là 5
+ Đặt Account lockout duration là 5
+ Đặt Reset account lockout counter after là 5

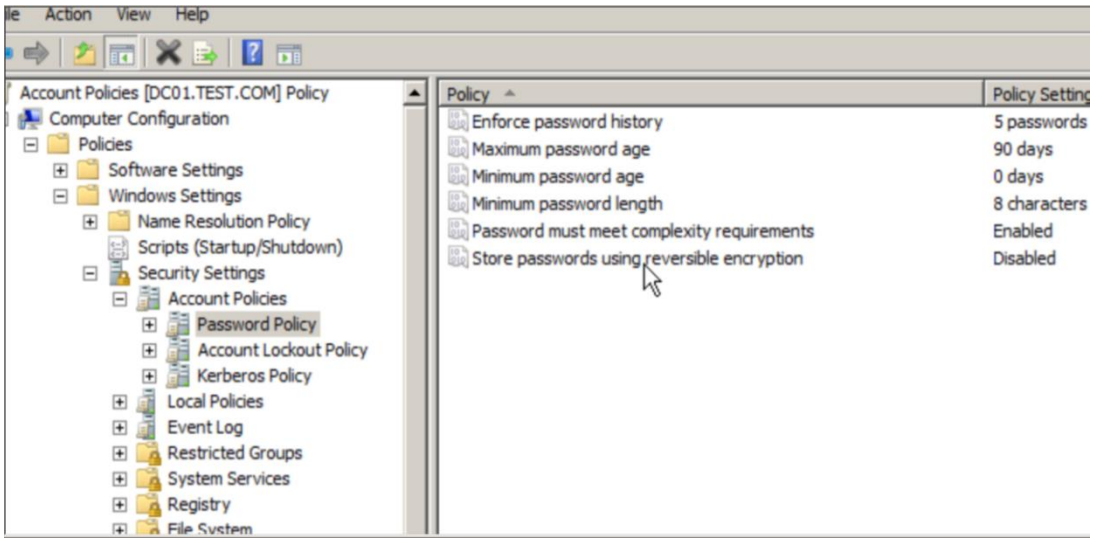


5.3. Chính sách về mật khẩu

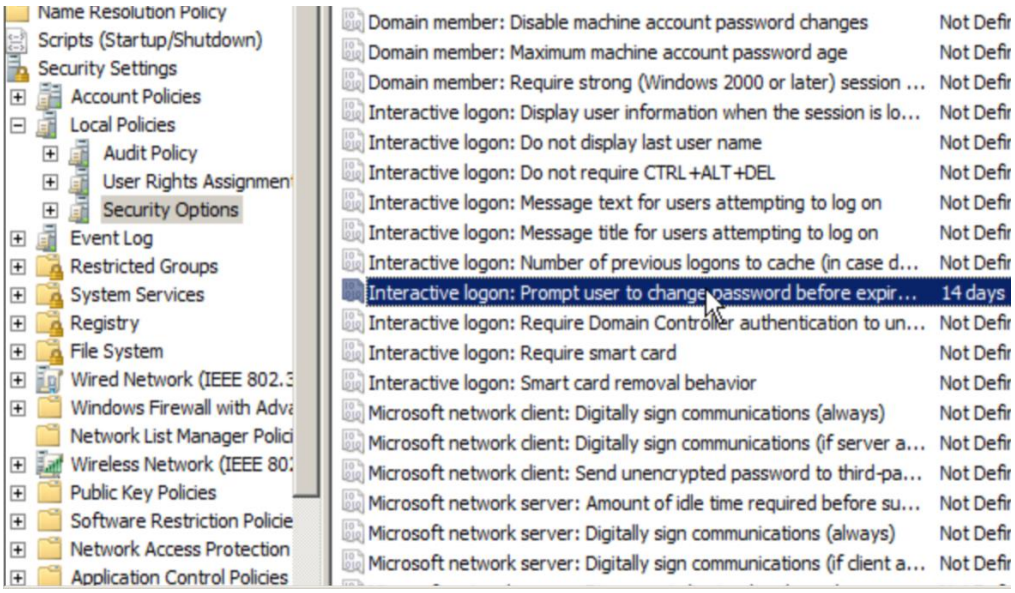
- Start -> gõ ” Group Policy Management” -> Chuột phải vào tên domain và chọn ”Create a GPO in this domain, and Link it here” -> Tạo 01 GPO tên là “Domain Policy” -> Ok để tạo GPO thiết lập tất cả các chính sách chung cho toàn Domain

- Click chuột phải vào GPO “Domain Policy” -> Edit -> Mở tới Computer Configuration/ Policies/ Windows Settings/ Security Settings/ Account Policies/ Password Policy -> thiết lập các giá trị:

+ Đặt Enforce password history là 5
+ Đặt Maximum password age là 90
+ Đặt Minimum password age là 0
+ Đặt Minimum password length là 8
+ Đặt Password must meet complexity requirements là Enabled
+ Đặt Store passwords using reversible encryption là Disabled

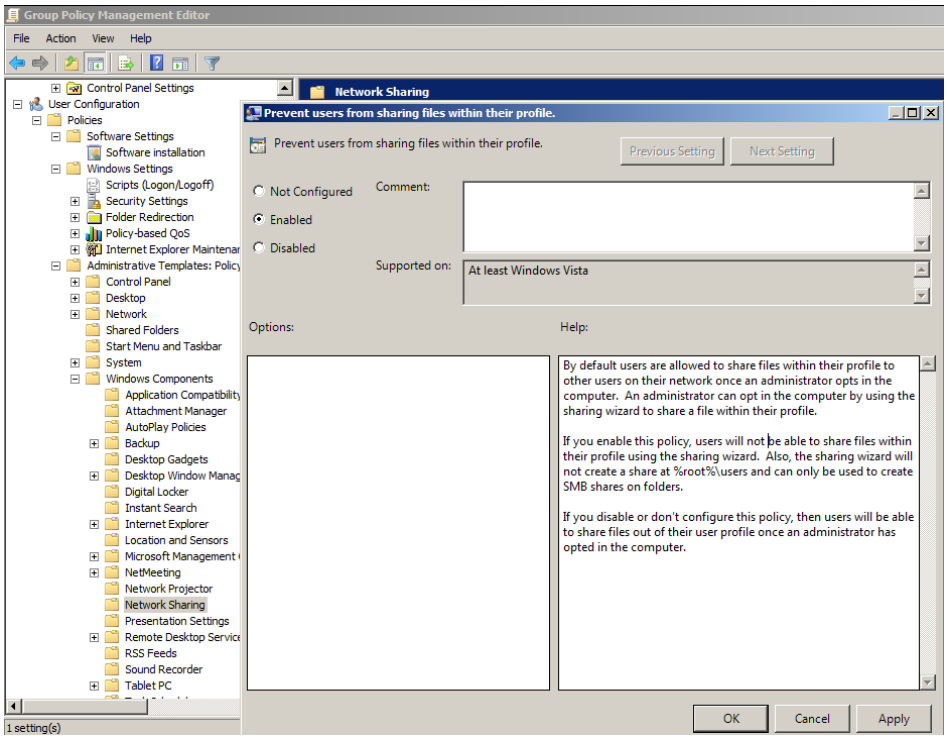


- Chuyển sang ”Security Options” -> Thiết lập ”Interactive logon: Promt user to change password before expiration” giá trị 14



6. Tắt chia sẻ mặc định

- Click chuột phải vào GPO "Domain Policy" -> Edit -> Mở tới Computer Policy -> User Configuration -> Administrative Templates -> Windows Components -> Network Sharing -> Click chọn "Prevent users from sharing files within their profile" chọn "**Enabled**"



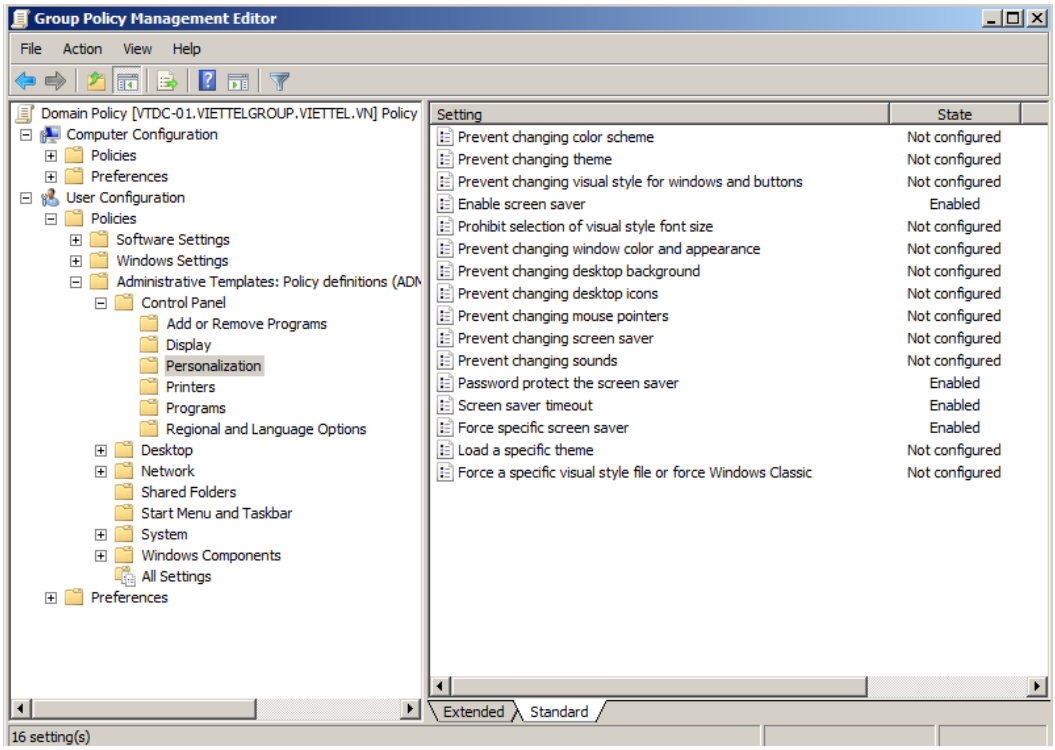
7. Chính sách khóa màn hình sau 5 phút không sử dụng

- Click chuột phải vào GPO "Domain Policy" -> Edit -> User Configuration/ Policies/ Administrative Templates/Control Panel/Persionalization

+ Đặt Enable screen saver và Password protect the screen saver là Enabled

+ Đặt Screen saver timeout là Enabled với giá trị là 300 (5 phút)

+ Đặt Force specific screen saver -> Enabled -> thêm câu lệnh để thực thi "**user32.dll,LockWorkStation**" vào trong Screen saver excutable name

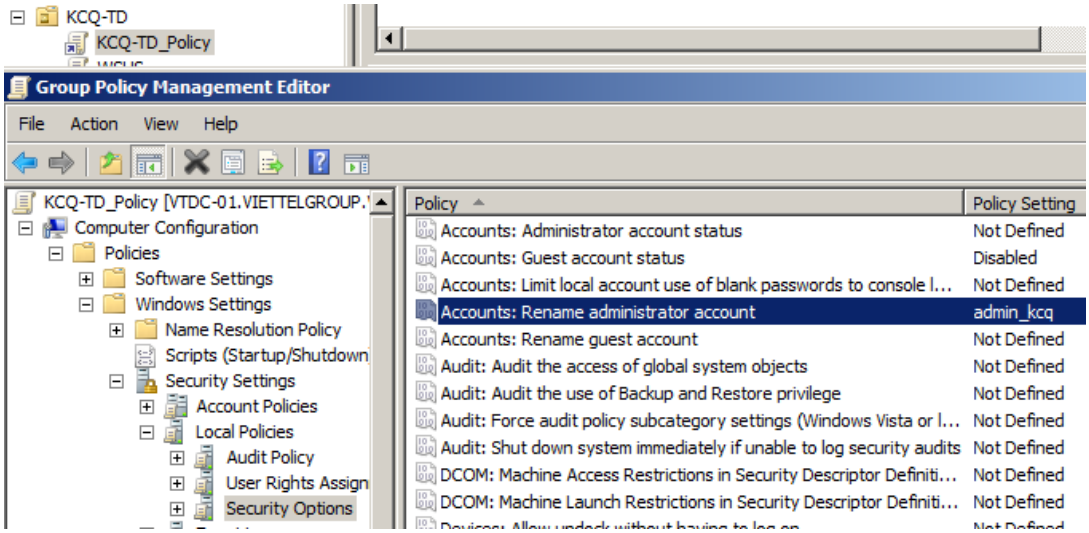


8. Thu hồi/đổi tên tài khoản Administrator Local và Disable tài khoản Guest

- Click chuột phải vào GPO cần áp dụng riêng cho OU các phòng/ban -> Edit -> Mở tới Computer Configuration/ Policies/ Windows Settings/ Security Settings/ Local Security/ Security Options

+ Click chọn "Accounts: Rename administrator account" -> Click chọn "Define this policy" -> đặt lại tên lại tài khoản Administrator.

+ Đặt Accounts: Guest account status là Disabled



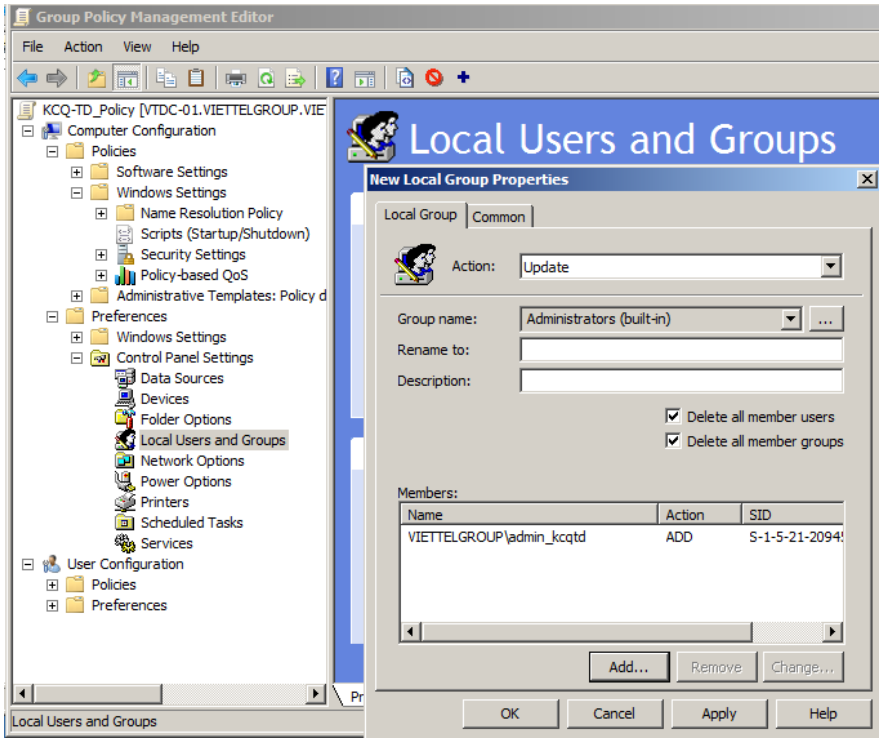
- Mở tới Computer Configuration/ Preferences/ Control Panel Settings/ Local Users and Groups -> Chuột phải chọn New/ New Group

+ Group Name -> chọn Administrators (built –in)

+ Action -> Chọn Update

+ Click chọn Delete all member users và Delete all member groups

+ Click chọn add và thêm các user (hoặc group) được quyền quản trị tại các máy client trong domain đối với OU đó.

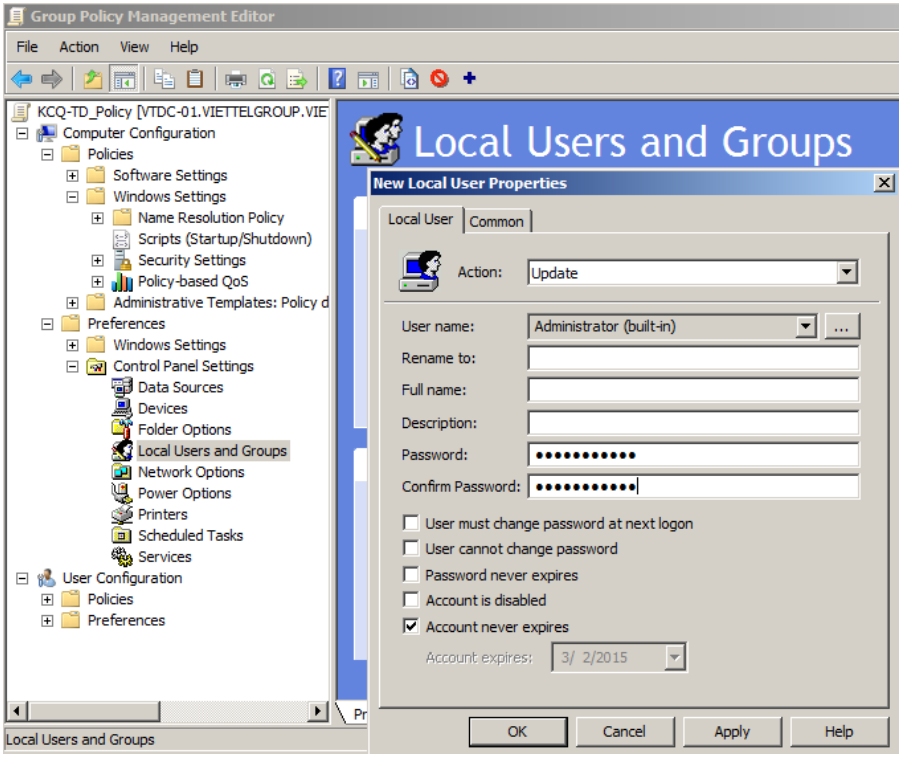


- Thiết lập mật khẩu cho tài khoản Administrator Local: Click chuột phải chọn New/ Local User.

+ Group Name -> chọn Administrators (built –in)

+ Action -> Chọn Update

+ Đặt mật khẩu cho tài khoản Administrator Local của các máy trạm theo từng OU đơn vị có đầu mối CNTT được ủy quyền quản trị -> Apply -> Ok



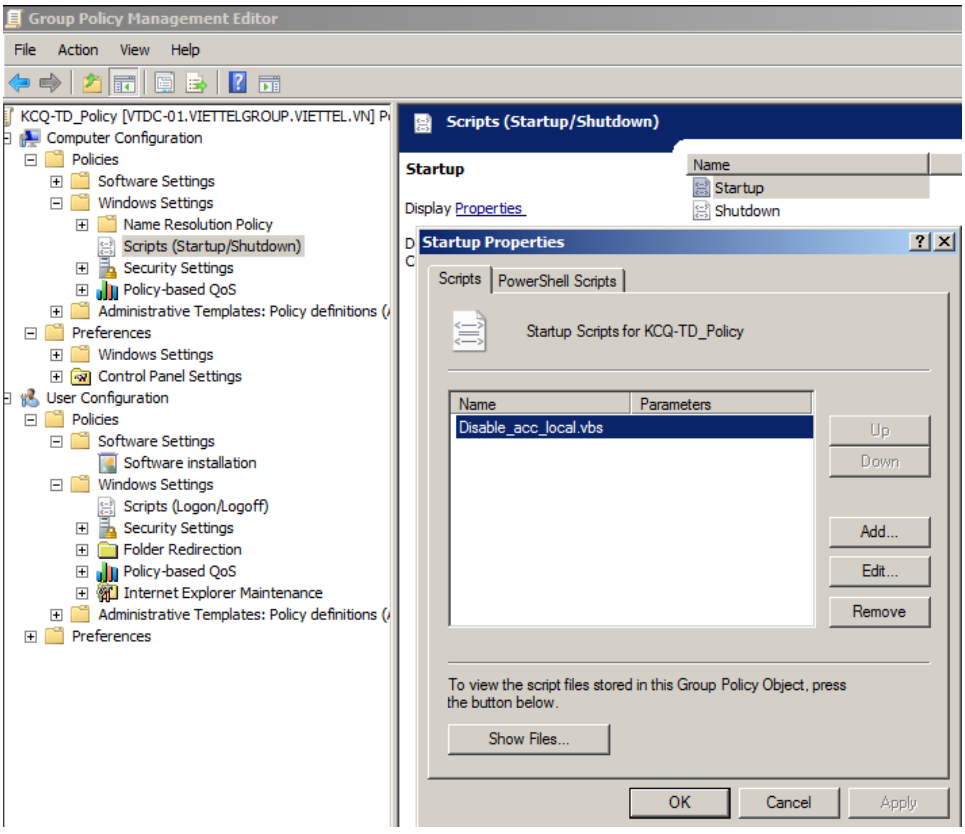
- Disable các tài khoản local trên máy tính người dùng loại trừ một số tài khoản:

+ Lưu đoạn code sau thành file Disable_acc_local.vbs

```
'*****************************************************
' File:  Disable Local User Accounts.vbs
' Author: Andrew Barnes
' version:  1.0 Date: 07 September 2009 By : Andrew D Barnes
' Lists local accounts and disables all except local Administrator and ASPNET
'*****************************************************
 Set objShell = CreateObject("Wscript.Shell")
Set objNetwork = CreateObject("Wscript.Network")
 strComputer = objNetwork.ComputerName
 Set colAccounts = GetObject("WinNT://" & strComputer & "")
 colAccounts.Filter = Array("user")
 Message = Message & "Local User accounts:" & vbCrLf & vbCrLf
 For Each objUser In colAccounts
 If objUser.Name <> "Administrator" AND objUser.Name <> "ASPNET" Then
        Message = Message & objUser.Name
```

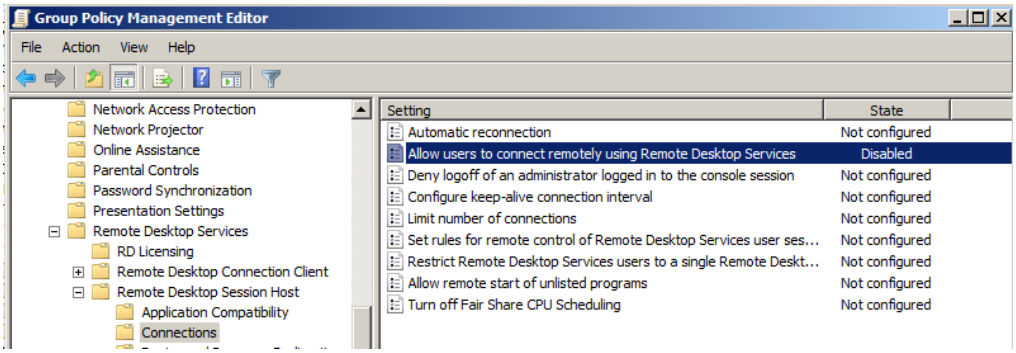
```
        If objUser.AccountDisabled = TRUE then
            Message = Message & " is currently disabled" & vbCrLf
        Else
            Message = Message & " was enabled" & vbCrLf
            objUser.AccountDisabled = True
            objUser.SetInfo
        End if
    End If
  Next
  ' Initialize title text.
 Title = "Local User Accounts By Andrew Barnes"
 objShell.Popup Message, , Title, vbInformation + vbOKOnly
```

- Click chuột phải vào GPO "Domain Policy" -> Edit -> mở tới Computer Configuration/Policies/Windows Settings/Scripts -> Startup -> Chọn Show Files và copy file **Disable_acc_local.vsb** vào thu mục Startup -> Chọn Add -> Chọn File **Disable_acc_local.vbs** -> Browse tới File **Disable_acc_local.vbs** trong thư mục Startup -> Open -> Ok -> Apply -> Ok

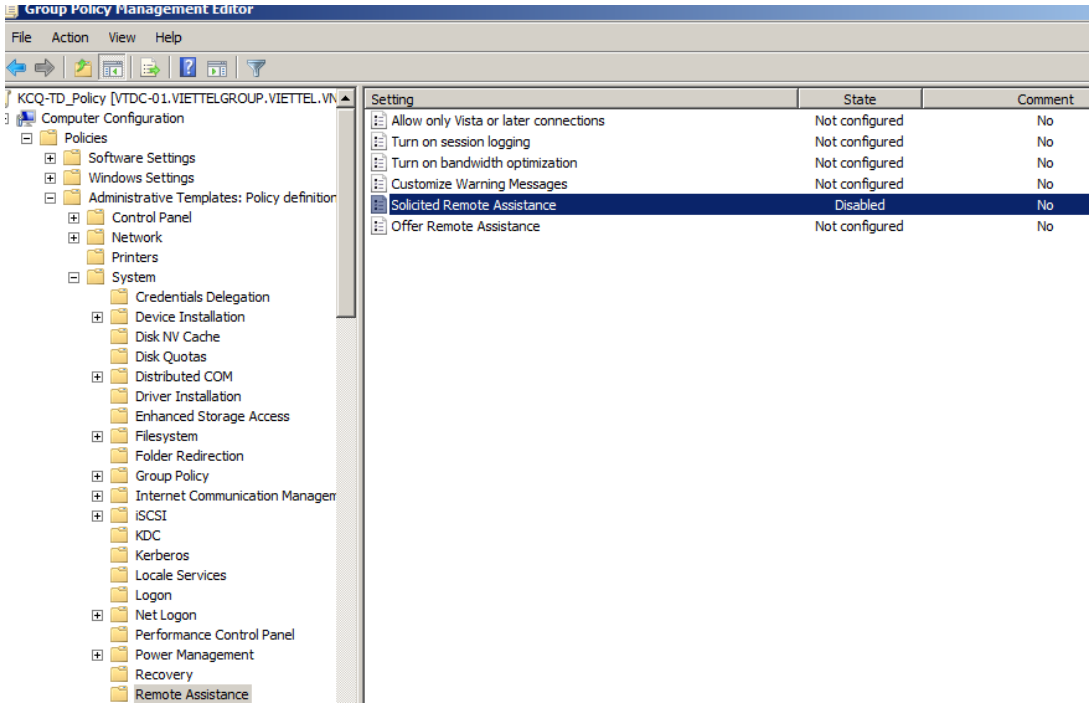


9. Tắt tính năng Remote Desktop, Remote Assistance cho máy tính người dùng

- Start -> gõ ” Group Policy Management” -> Click chuột phải vào GPO “Domain Policy” -> Edit -> Computer Configration/ Policies/Administrative Template/Window Components/Remote Desktop Services/Remote Desktop Session Host/Connections (trên Windows Server 2008 là Computer Configration/ Policies/Administrative Template/Window Components/Terminal Services/Terminal Server/Connections) -> Thiết lập Allow users to connect remotely using Remote Desktop Services (trên Windows Server 2008 là Allow users to connect remotely using Terminal Services) giá trị “Disabled” -> Ok



- Start -> gõ ” Group Policy Management” -> Click chuột phải vào GPO “Domain Policy” ->Computer Configuration\Policies\Administrative Templates\System\Remote Assistance -> Thiết lập Solicited Remote Assistance giá trị “Disabled”

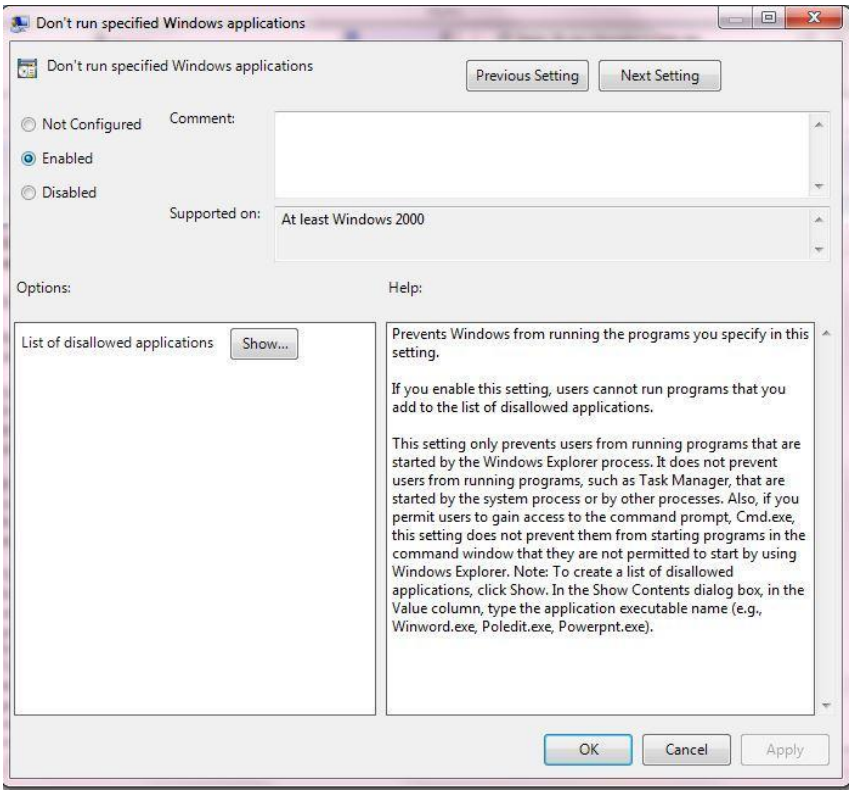


10. Tắt chế độ Auto-Run đối với các ổ cứng, ổ lưu trữ di động, ổ CD-ROM

- Mở tới Computer Configration/ Policies/ Administrative Template/Window Components/AutoPlay Policies -> Thiết lập Turn off Autoplay giá trị Enabled -> OK

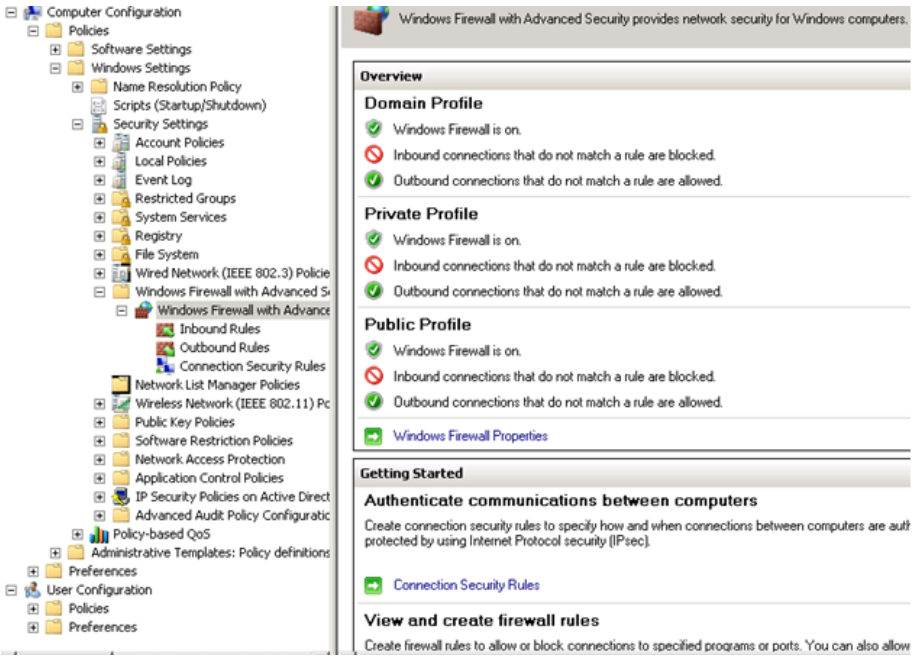
11. Chặn phần mềm chat client như: Yahoo Messenger, Skype, Google Talk, MSN chat, Teamviewer, Logmein, VNC, Radmin, X-manager

- Click chuột phải vào GPO "Domain Policy" -> Edit -> User Configration/ Policies/Administrative Template/System -> Thiết lập giá trị Don't run specified Windows applications là Enabled -> trong phần List of disallowed applications chọn Show -> nhập các tên tiến trình không cho phép -> Ok -> Ok

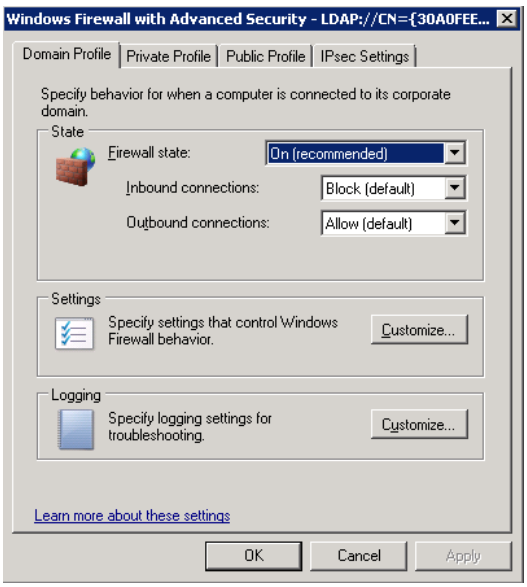


12. Bật tường lửa windows và cấu hình giới hạn truy cập ngang hàng

- Click chuột phải vào GPO "Domain Policy" -> Edit -> Computer Configuration -> Policy -> Windows Settings -> Security Settings -> Windows Firewall with Advance Security



- Click chuột phải vào Windows Firewall with Advance Security -> chọn Properties



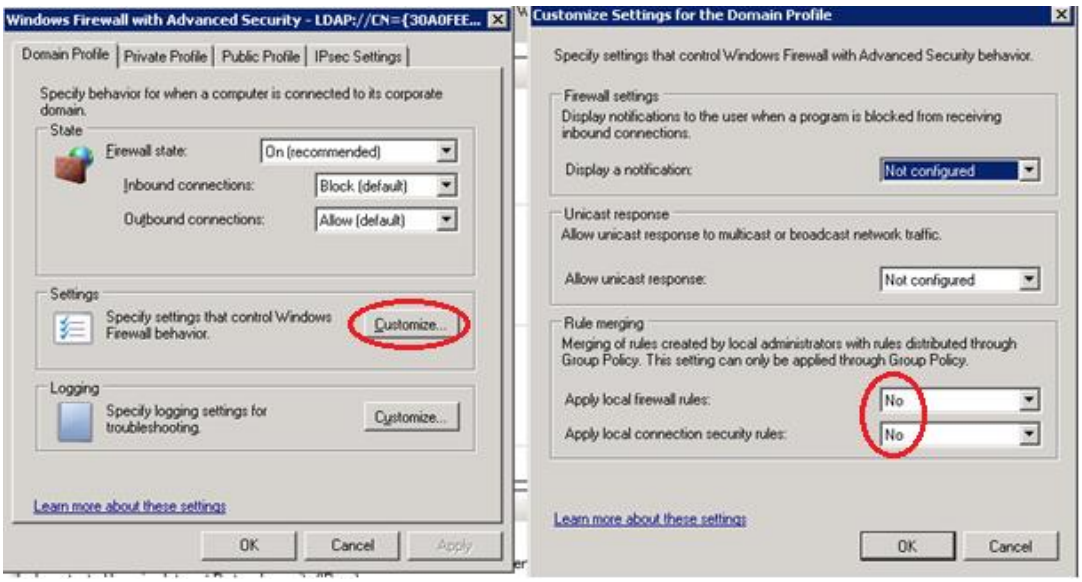
- Thực hiện các thiết lập như sau trên cả Domain, Private, Public Profile

+ Firewall state: On (Để bật Windows Firewall)

+ Inbound connections: Block (default) (Mặc định chặn kết nối chiều vào)

+ Outbound connection: Allow (default) (Mặc định cho phép kết nối chiều ra)

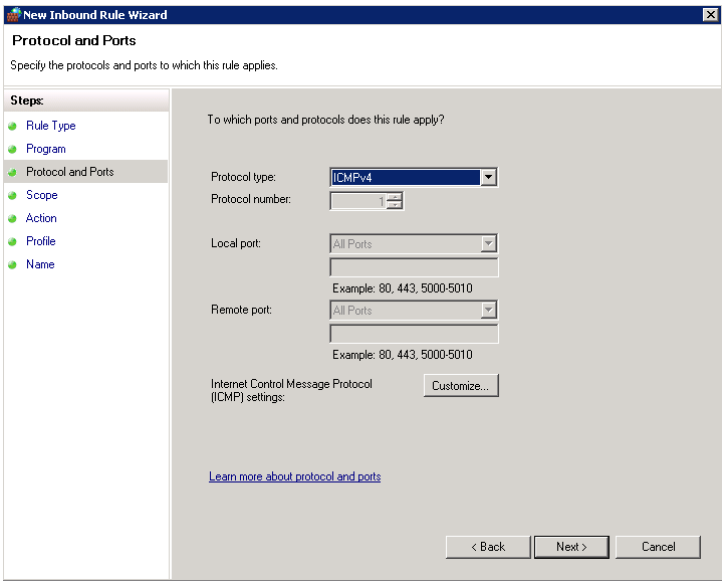
+ Click Customize trong Settings -> chọn No trong Apply local firewall rules -> Apply local connection security rules (Để disable tất cả những luật đã có sẵn trên máy tính người dùng, chỉ áp dụng những luật đẩy từ Group Policy)



+ Click OK để áp dụng thiết lập.

- Tạo luật trong Inbound rule thêm các luật sau:

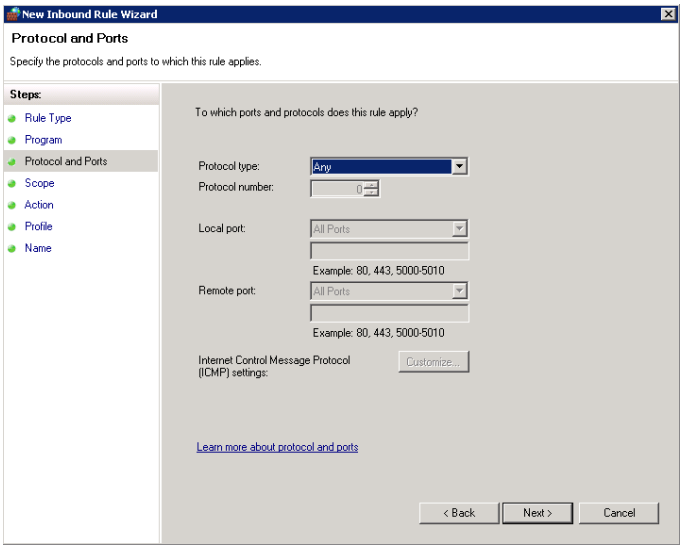
+ Luật 01: Cho phép Ping: Click chuột phải -> New rules -> trong Rule Type chọn Custom -> Next -> trong Program chọn All programs -> Next -> rong Protocol and Ports chọn Protocol type: ICMPv4 -> Next



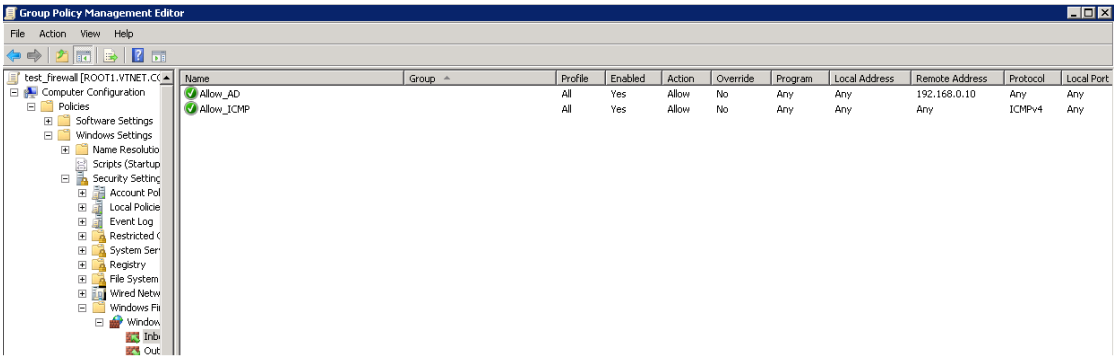
Trong phần Scope để mặc định -> Next -> Trong phần Action chọn Allow the connection -> Next -> Trong phần Profile tích chọn 3 profile: Domain, Private, Public -> Trong phần Name: Đặt tên cho policy - Finish

+ Luật 02: Cho phép kết nối từ AD

Click chuột phải -> New rules -> Trong Rule Type chọn Custom -> Next -> Trong Program chọn All programs -> Next -> Trong Protocol and Ports chọn Protocol type: ICMPv4 -> Next

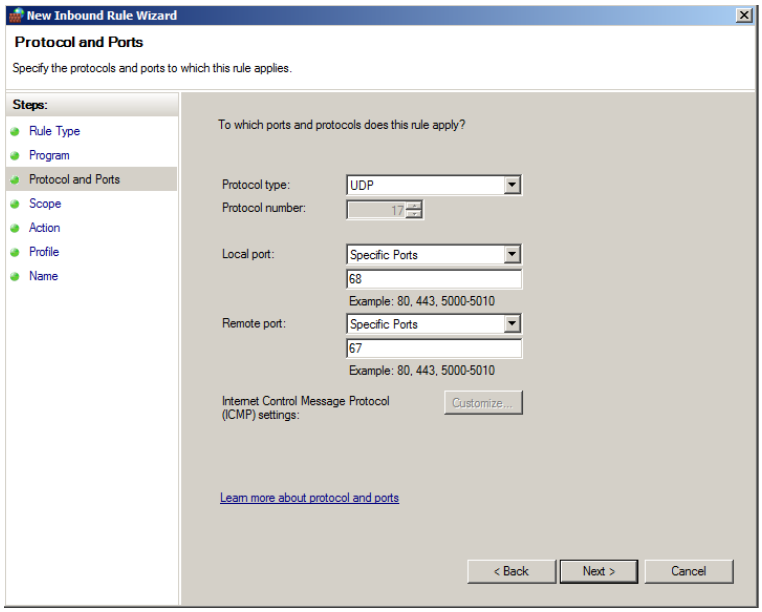


Trong phần Scope đặt lại địa chỉ của AD trong phần Remote IP Address -> Trong phần Action chọn Allow the connection -> Next -> Trong phần Profile tích chọn 3 profile: Domain, Private, Public -> Trong phần Name: Đặt tên cho policy – Finish



Trong trường hợp có sử dụng DHCP thì cần tạo thêm 1 luật cho phép nhận gói tin từ DHCP server như sau:

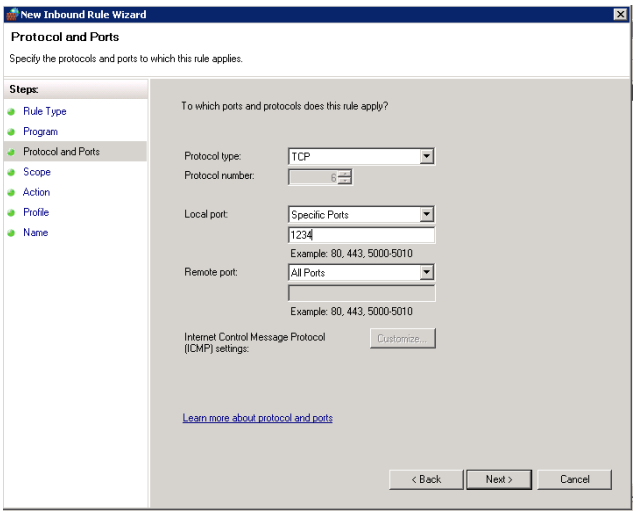
Trong phần Protocol and Ports thì Protocol type: UDP, Local port 68 và Remote port là 67.



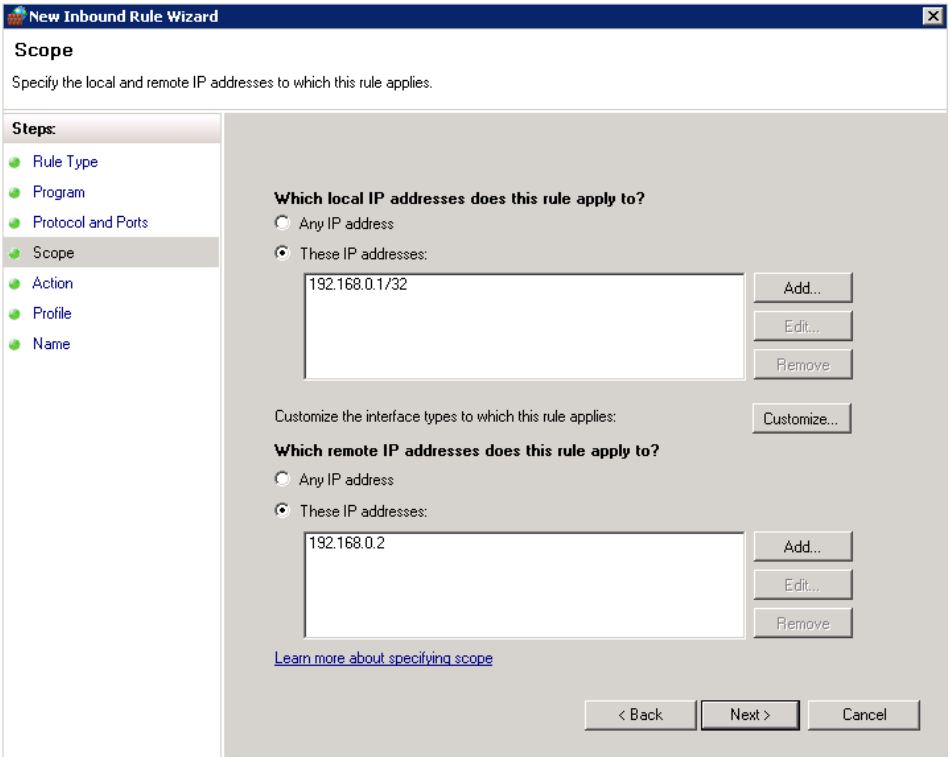
Đối với trường hợp ngoại lệ thì cần tạo luật chỉ rõ cổng kết nối trong phần Protocol, địa chỉ nguồn trong phần Remote address và địa chỉ đích trong phần Local address.

Ví dụ: nếu muốn cấu hình cho phép 1 máy tính 192.168.0.2 truy cập được đến máy tính 192.168.0.1 cổng TCP 1234 thì tạo luật như sau:

Trong Protocol and Ports chọn TCP, Local port chọn 1234



Trong phần scope, chỉ rõ Local Address là IP 192.168.0.1, Remote address là IP 192.168.0.2



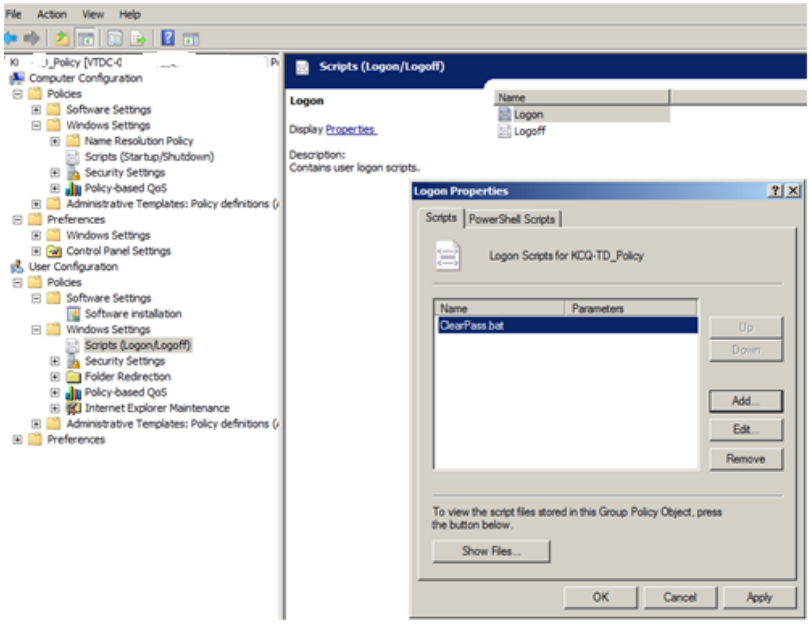
13. Xóa mật khẩu lưu trên trình duyệt

- Lưu đoạn text sau vào file tên ClearPass.bat

```
@echo off
```

```
\\ Xoa Password trong Chrome
set ChromeDirXP=%USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\Default\Login Data
set ChromeDir1XP=%USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache
del /q /s /f "%ChromeDirXP%"
rd /s /q "%ChromeDirXP%"
del /q /s /f "%ChromeDir1XP%"
rd /s /q "%ChromeDir1XP%"
\\ Trong Windows 7
set ChromeDir7=%USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Login Data
del /q /s /f "%ChromeDir7%"
\\
\\ Xoa cache trong Firefox
pushd %USERPROFILE%\Local Settings\Application Data\Mozilla\Firefox\Profiles\*.default\
del Cache\*.* /q
del OfflineCache\*.* /q
popd
\\ Trong Windows 7
pushd %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\*.default\
del signons.sqlite /q
popd
```

- Click chuột phải vào GPO "Domain Policy" -> Edit -> mở tới User Configuration/Policies/Windows Settings/Scripts -> Logon -> Chọn Show Files và copy file ClearPass.bet vào thu mục Logon -> Chọn Add -> Chọn File ClearPass.bat -> Browse tới File ClearPass.bat trong thư mục Logon -> Open -> Ok -> Apply -> Ok



14. Bật tính năng Cập nhật của Windows

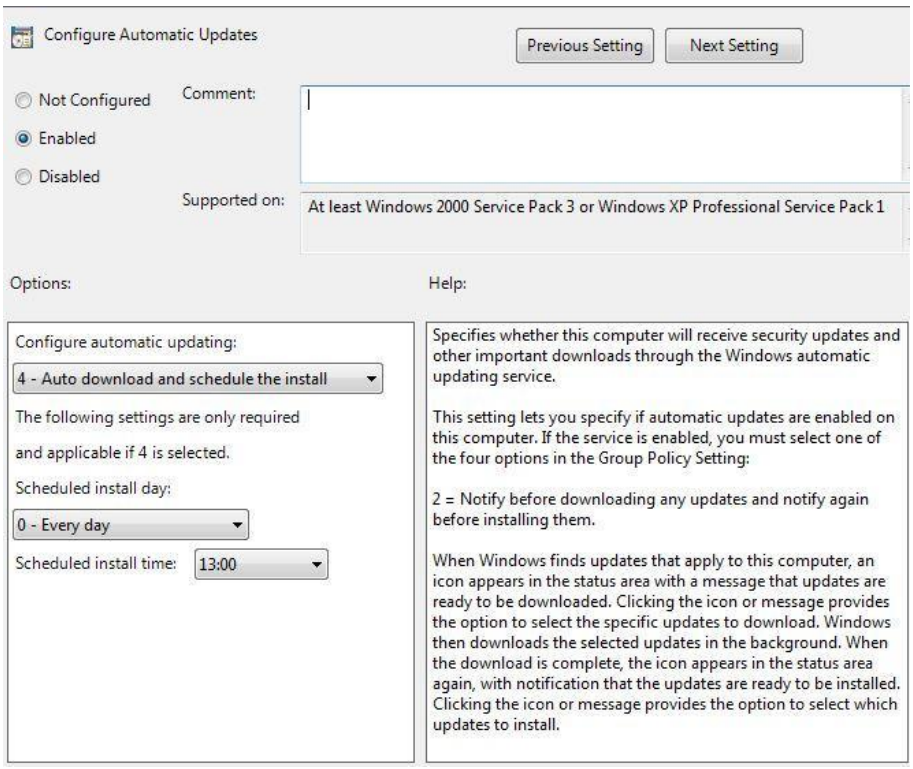
- Click chuột phải vào GPO "Domain Policy" -> Edit -> Mở tới Computer Configration/ Policies/Administrative Template/Window Components/Windows Update

+ Đặt Configure Automatic Updates là Enabled

+ Trong phần Configure automatic updating, chọn mục 4

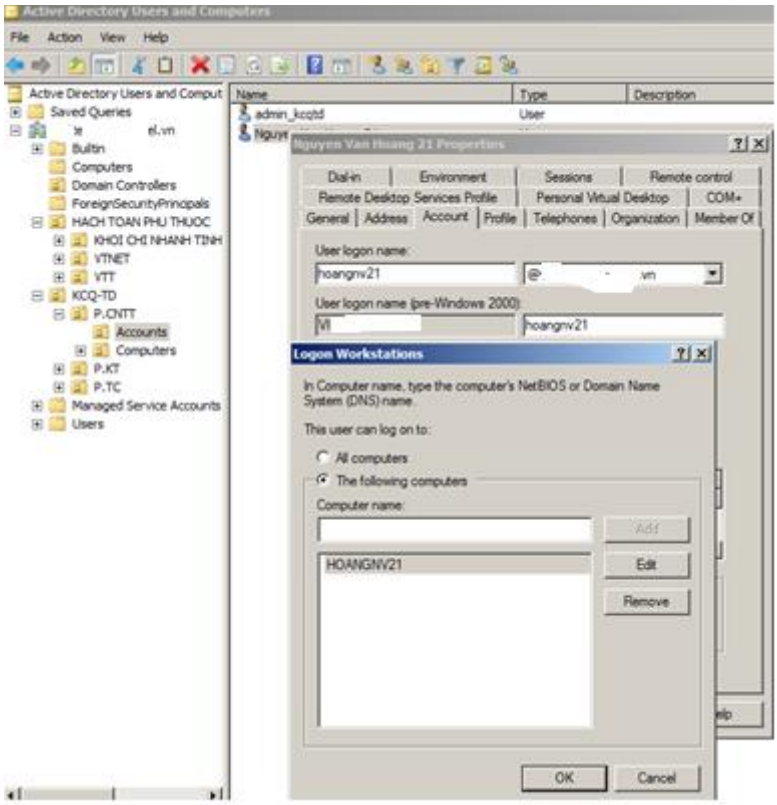
+ Trong phần Scheduled install day, chọn mục 0

+ Trong phần Scheduled install time, chọn thời gian để cài bản cập nhật hàng ngày -> Ok



15. Giới hạn máy đăng nhập của người dùng, mỗi tài khoản chỉ được đăng nhập vào các máy tính cho phép.

- Start -> gõ ” Active Directory Users and Groups ” Click chuột phải lên tài khoản người dùng -> Properties -> Chọn tab Account -> Log On to -> Chọn The following computers -> nhập tên máy và ấn -> Add -> OK



- Khi cần làm hàng loạt với 1 danh sách tài khoản có sẵn
  + Chỉnh sửa đoạn code sau

```
# Import-CSV C:\assign.csv | % {
# Author - Santhosh Sivarajan
#
Clear
Import-CSV C:\assign.csv | % {
$UserN = $_.UserName
$ComputerN = $_.ComputerName
$ObjFilter = "(&(objectCategory=person)(objectCategory=User)(samaccountname=$UserN))"
$objSearch = New-Object System.DirectoryServices.DirectorySearcher
$objSearch.PageSize = 15000
```

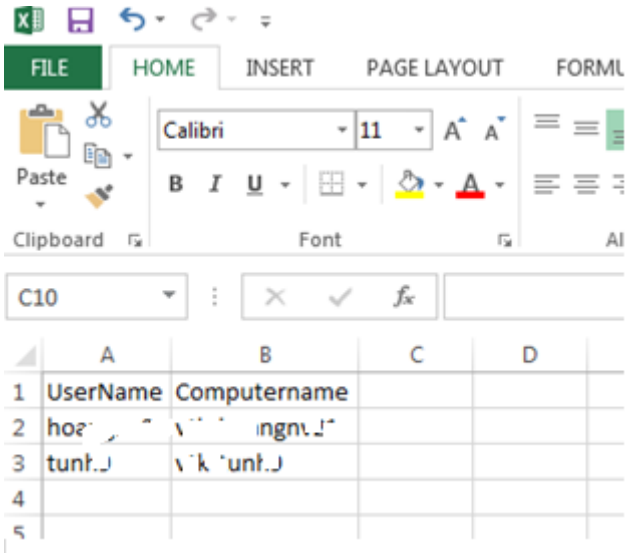
```
$objSearch.Filter = $ObjFilter
$objSearch.SearchRoot = "LDAP://dc=XYZ,dc=vn"
$AllObj = $objSearch.findOne()
$user = [ADSI] $AllObj.path
$ErrorActionPreference = "silentlycontinue"
If (($user.get("userWorkstations")) -ne $null)
{$ComputerN = $user.get("userWorkstations")+","+ $ComputerN}
Write-host -NoNewLine "Updating $UserN Properties ..."
$user.psbase.invokeSet("userWorkstations",$ComputerN)
Write-host "Done!"
$user.setinfo()
}
```

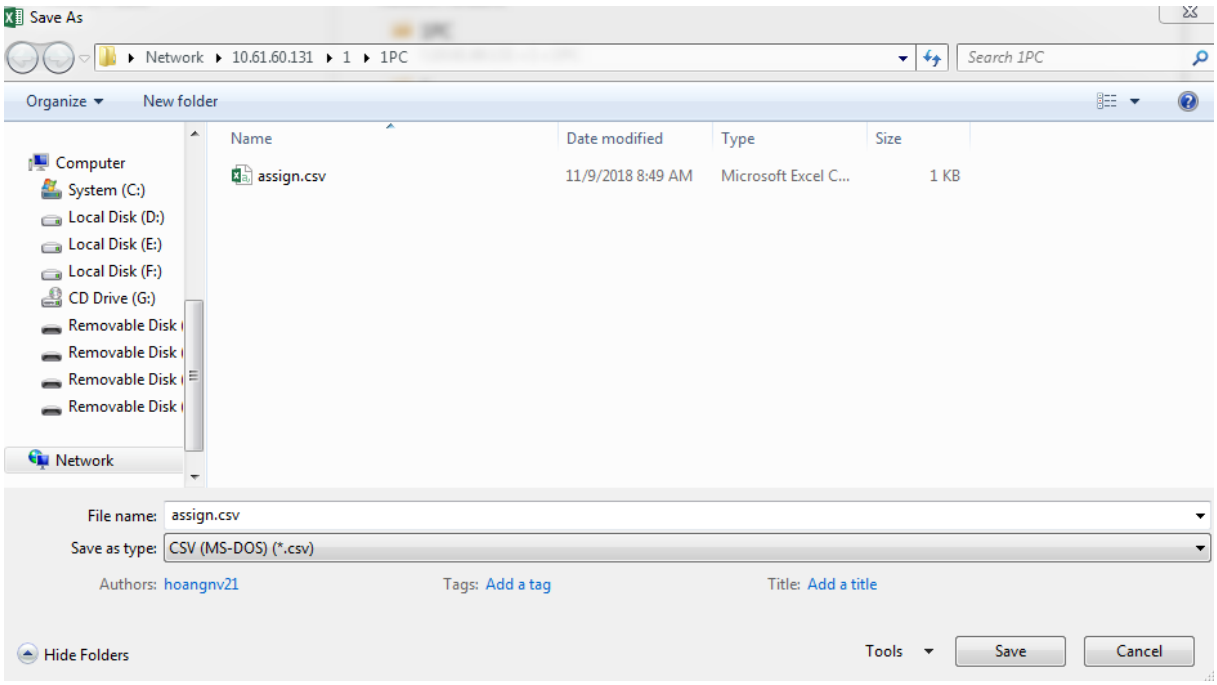
C:\assign.csv sửa thành đường dẫn tới file *assign.csv* lưu danh sách user và computer như bên dưới – Đây là file chỉ ra máy mà mỗi user được dùng (Nếu một người được đăng nhập vào nhiều máy thì ghi thành nhiều dòng)

LDAP://dc=XYZ,dc=vn là domain vttek.vn.

Save lại thành file assigning.ps1

Tạo 1 file excel chứa tên người dùng và tên máy như mẫu.

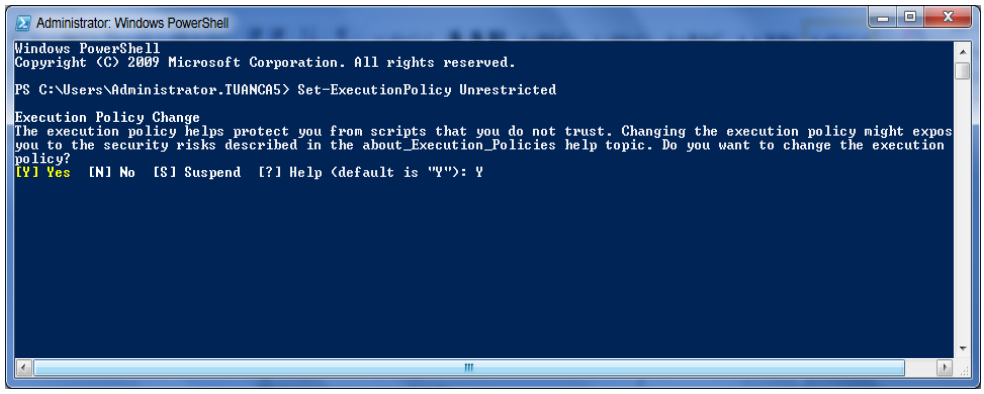




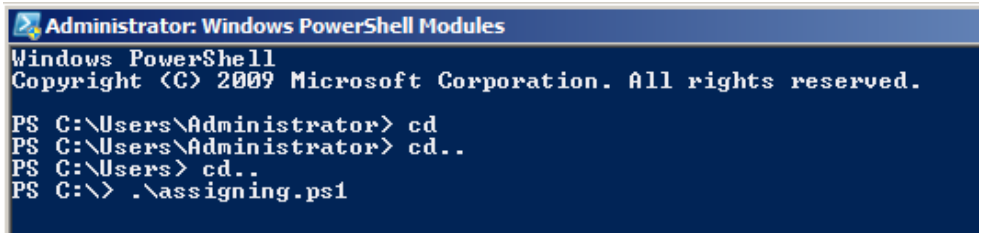
Save as thành file định dạng assign.csv [chú ý đuôi file CVS (MS-DOS) (*.csv)].

Mở Windows PowerShell (Cần mở dưới quyền admin)

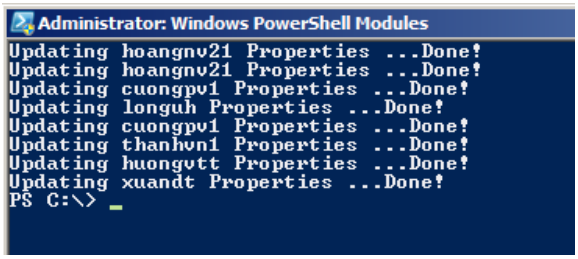
Gõ lệnh Set-ExecutionPolicy Unrestricted , ấn Y và Enter



Trỏ đường dẫn tới file assigning.ps1 và chạy lệnh .\assigning.ps1



Kết quả báo hoàn thành



Ghi chú: *Trường hợp đặc biệt cho phép nhiều tài khoản đăng nhập trên một máy tính: Máy tính phục vụ giám sát NOC, máy tính của điện thoại viên CSKH,…*

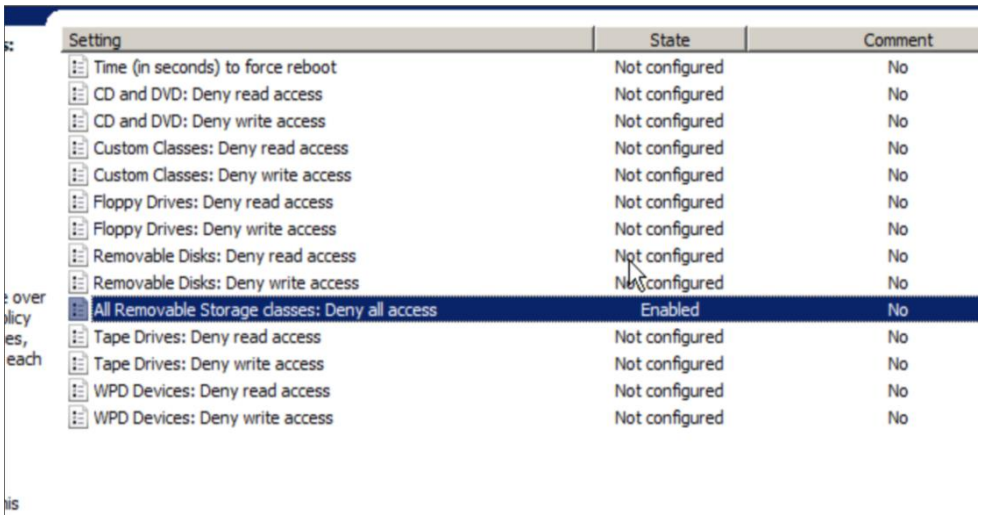
16. Ngắt thiết bị lưu trữ, đọc ghi dữ liệu

- Vào Start -> gõ ” Group Policy Management” Click chuột phải vào GPO cần áp dụng cho đơn vị -> Edit -> mở tới User Configuration/ Policies/ Administrative Templates/ System/ Removable Storage Access

+ Nếu muốn chặn USB (flash driver) thì đặt Removable Disks: Deny read access và Removable Disks: Deny write access là Enabled

+ Nếu muốn chặn ổ đĩa CD và DVD thì đặt CD and DVD: Deny read access và CD and DVD: Deny write access là Enabled

+ Nếu muốn chặn tất cả các thiết bị lưu trữ ngoài thì đặt All Removable Storage classes: deny all access là Enabled



Phụ lục 02.
HƯỚNG DẪN LẬP TRÌNH AN TOÀN TRONG PHÁT TRIỂN ỨNG DỤNG WEB TRÊN FRAMEWORK .NET

1. Quản lý xác thực

- ***Thông tin định danh***

1.1. Tên đăng nhập phải là duy nhất, chỉ nên chứa tập các ký tự là chữ cái, chữ số, dấu gạch dưới

```
public static Boolean isExistUsername(string username)
      {
         using (SqlConnection con = new SqlConnection("Data Source=etc"))
         {
            bool isExist = false;
            con.Open();
            using (SqlCommand cmd = new SqlCommand("select count(*) 
from [User] where UserName = @UserName", con))
            {
               cmd.Parameters.AddWithValue("UserName", username);
               isExist = (int)cmd.ExecuteScalar() > 0;
            }
            con.Close();

            // return result
            return isExist;
         }
      }

public static Boolean isValidUsername(string username)
      {
         if (username == null || username.Equals(""))
         {
            return false;
         }
         else
```

```
            return Regex.IsMatch(username, "^(?=.{6,30}$)[a-zA-Z0-9._]+$");
        }
```

1.2. Thiết lập chính sách mật khẩu mạnh

- Mật khẩu có độ dài tối thiểu là 10 ký tự.
- Chứa chữ cái, chữ số và kí tự đặc biệt.
- Thiết lập blacklist các mật khẩu yếu (VD: 123456A@, 123456a@,…).

```
public static Boolean isStrongPassword(string password)
        {
            if (password == null)
                return false;
            else
                return Regex.IsMatch(password, "^((?=(.*[a-zA-
Z]){1,})(?=(.*[\\d]){1,})(?=(.*[\\W]){1,})(?!.*\\s)).{8,}$")
                    && !isBlacklistPassword(password);
        }


private static Boolean isBlacklistPassword(string password)
        {
            string path = @"d:\password_blacklist.txt";
            string[] fileText = File.ReadAllLines(path);
            foreach (var text in fileText)
            {
                if (password.Equals(text))
                    return false;
            }
            return true;
        }
```

1.3. Thiết lập thời gian hết hiệu lực cho mật khẩu tối đa 90 ngày, mật khẩu mới không được trùng với mật khẩu hiện tại.

1.4. Đối với chức năng reset/ quên mật khẩu:

- Đường dẫn reset/quên mật khẩu được gửi qua email phải bị mất hiệu lực sau lần truy cập đầu tiên hoặc sau 8 giờ nếu không được truy cập.

- Nếu chức năng reset/quên mật khẩu thực hiện gửi mật khẩu qua email thì mật khẩu phải được sinh ngẫu nhiên và phải tuân theo chính sách mật khẩu mạnh tại mục 2.

1.5. Chỉ lưu dạng mã hash của mật khẩu trong DB (khuyến nghị thuật toán hash là SHA-256), thêm chuỗi salt ngẫu nhiên vào mật khẩu trước khi thực hiện hash.

```
public enum HashType : short
    {
       [DescriptionAttribute("SHA1CryptoServiceProvider")]
       SHA1 = 0,
       [DescriptionAttribute("SHA256Managed")]
       SHA256 = 1,
       [DescriptionAttribute("SHA384Managed")]
       SHA384 = 2,
       [DescriptionAttribute("SHA512Managed")]
       SHA512 = 3
    }

    // Creates a random salt to add to a password.
    public static string CreateSalt()
    {
       RandomNumberGenerator rng = RandomNumberGenerator.Create();
       byte[] number = new byte[32];
       rng.GetBytes(number);
       return Convert.ToBase64String(number);
    }

    // Creates the password hash using a given HashType algorithm.
    public static string CreatePasswordHash(string salt, string password,
HashType hashType)
    {
       string hashString = string.Empty;
       if (!string.IsNullOrEmpty(password))
```

```
        {
            HashAlgorithm hashAlg =
HashAlgorithm.Create(hashType.ToString());
            byte[] pwordData = Encoding.Default.GetBytes(salt + password);
            byte[] hash = hashAlg.ComputeHash(pwordData);
            hashString = Convert.ToBase64String(hash);
        }
        return hashString;
    }

    // Creates the password hash using SHA256 managed hash algoritm.
    public static string CreatePasswordHash(string salt, string password)
    {
        return CreatePasswordHash(salt, password, HashType.SHA256);
    }
```

➢ ***Xử lý xác thực***

1.1. Trả về thông báo chung cho trường hợp người dùng đăng ký thông tin định danh (username, email,…) đã tồn tại tại chức năng đăng ký, hoặc gửi sai thông tin định danh tại các chức năng đăng nhập, reset/quên mật khẩu, đổi địa chỉ email…

1.2. Bật cơ chế bảo vệ bằng Captcha hoặc các hình thức tương đương khi đăng nhập sai quá 5 lần liên tiếp. Cần triển khai cơ chế này tại các chức năng quan trọng khác của ứng dụng.

- Sử dụng Captcha an toàn theo Chỉ thị sử dụng Captcha an toàn Tập đoàn đã ban hành.
- Thực hiện kiểm tra tính hợp lệ của Captcha trước khi thực hiện chức năng được request.

1.3. Chỉ sử dụng phương thức POST để submit thông tin định danh, khuyến nghị sử dụng HTTPS cho đường truyền để tăng tính bảo mật.

2. Quản lý phiên đăng nhập

2.1. Session phải được quản lý bởi server, sinh ngẫu nhiên và độ dài tối thiểu là 128 bit.

2.2. Session phải được thiết lập thời gian timeout, giá trị timeout cần cân bằng giữa nhu cầu thương mại và yếu tố bảo mật.

Thiết lập cấu hình timeout tại file W***eb.config***:

```
<configuration>
  <system.web>
    <sessionState
      mode="InProc"
      cookieless="true"
      timeout="30" />
  </system.web>
</configuration>
```

2.3. Tạo mới session sau khi đăng nhập thành công.

2.4. Xóa giá trị sessionid và các dữ liệu gắn với session đó khi người dùng đăng xuất.

- Đối với cả 2 trường hợp 2.3 và 2.4, .Net hỗ trợ hàm Session.Abandon() thực hiện việc xóa sessionId và toàn bộ dữ liệu lưu trên sessionId đó. Khi client submit lên sessionId không còn tồn tại trên server, server sẽ tự động sinh 1 sessionId mới và trả về cho client.

```
// sau khi đăng nhập thành công hoặc đăng xuất gọi hàm
Session.Abandon();
```

2.5. Cấu hình thuộc tính "Secure" đối với các ứng dụng sử dụng HTTPS và "HTTP-Only" cho trường session cookie.

- Cấu hình thuộc tính "Secure" trong file ***Web.config***:

```
<system.web>
<httpCookies domain="" httpOnlyCookies="true" requireSSL="true" />
</system.web>
```

- Cấu hình "HTTP-Only" trong file ***Web.config***:

```
<system.web>
<httpCookies domain="" httpOnlyCookies="true" requireSSL="true" />
</system.web>
```

2.6. Đối với các chức năng quan trọng có tương tác với database, ứng với mỗi phiên cần sinh thêm 1 token ngẫu nhiên, và thực hiện kiểm tra tính hợp lệ của token này trước khi xử lý truy vấn từ người dùng.

- Sử dụng cơ chế filter [ValidateAntiForgeryToken] được hỗ trợ trong MVC .Net như sau:

Ví dụ chức năng chính sửa thông tin tài khoản người dùng.

Bước 1: Gọi filter [ValidateAntiForgeryToken] trước hàm xử lý chức năng chỉnh sửa.

[ValidateAntiForgeryToken]

```
[HttpPost]
public ActionResult EditUser(int id, string Username, string Password, string Email)
{
   try
   {
      UserRegister user = new UserRegister();
      user.Id = id;
      user.UserName = Username;
      user.Password = Password;
      user.Email = Email;
      Repositories.updateUser(user);
      return Json(new { Type = "SUCCESS" });
   }
   catch (Exception e)
   {
   }
   return Json(new { Type = "ERROR" });
}
```

Bước 2: Tại trang view, sử dụng @Html.AntiForgeryToken() để tạo biến __RequestVerificationToken

```
<form id="msform">
   <!-- fieldsets -->
   <fieldset>
      <h2 class="fs-title" style="color: #3366FF">
         <img src="~/Content/images/user.png" style="margin-bottom: -20px" />THÔNG TIN CHI TIẾT</h2>
      <p style="font-size: 20px;">Username:</p>
      <input type="text" id="Username" name="Username" value="@Model.UserName" class="tb"/>
```

```
        <p style="font-size: 20px;">Password:</p>
        <input type="password" id="Password" name="Password"
value="@Model.Password" class="tb"/>
        <p style="font-size: 20px;">Email:</p>
        <input type="text" name="Email" id="Email" value="@Model.Email"
class="tb"/>
        <br />
        <input type="button" name="next" class="action-button" value="Cập
nhật" onclick="editUser();" />
        @Html.AntiForgeryToken()
        <p id="err"></p>
    </fieldset>
</form>
```

Trường hợp không sử dụng submit mà xử lý bằng jquery - ajax:

```
editUser = function () {
    var id = @Model.Id;
    var un = $("#Username").val();
    var pw = $("#Password").val();
    var em = $("#Email").val();
    var token = $("input[name=__RequestVerificationToken]").val()
    var kData = {"id":id,"username":un, "password":pw, "email":em,
"__RequestVerificationToken":token}
    $.ajax({
        url: '@Url.Action("EditUser", "Manager")',
        data: kData,
        type: 'POST',
        datatype: 'json',
        success: function (msg) {
            if (msg.Type == "SUCCESS") {
                /* jAlert("Thành công","Thông báo"); */
                }
                else {
                    $('#err').html("Có lỗi xảy ra!!!").css("color", "red");
                }
```

```
        }
    }
        );
    return false;
}
```

3. Phân quyền

3.1. Kiểm tra phân quyền dựa trên các đối tượng được lưu tại server (VD: tham số lưu trên session server, dữ liệu lưu trên DB,…).

3.2. Phân quyền tối thiểu, chỉ đáp ứng đủ chức năng và tài nguyên cho người dùng/ứng dụng.

3.3. Phía giao diện người dùng: Chỉ hiển thị các thành phần giao diện, đường dẫn, hàm,... tương ứng với quyền của người dùng.

3.4. Phía server: Kiểm tra quyền tác động của người dùng/ứng dụng trên các hàm và tài nguyên tương ứng trước khi thực hiện bất cứ tác vụ nào tới hệ thống.

3.5. Phải có tính năng xóa phiên làm việc hiện tại của người dùng hoặc các cơ chế tương đương đối với các trường hợp quyền người dùng bị thay đổi hoặc bị disable bởi người dùng có thẩm quyền.

3.6. Không đặt trang quản trị public internet, trong trường hợp bắt buộc phải đặt public cần giới hạn các IP được phép truy cập hoặc sử dụng cơ chế xác thực đa nhân tố (multiple authentications).

4. Tương tác với back-end

- Mã hóa các dữ liệu nhạy cảm trước khi lưu trữ (thông tin tài khoản ngân hàng, private key,..).

- Sử dụng thuật toán mã hóa AES, secret key lưu trữ trong file cấu hình đặt trên DB.

```
string credit = "creaditExample";
Aes myAes = Aes.Create();
myAes.GenerateKey();

byte[] key =
Encoding.UTF8.GetBytes(ConfigurationManager.AppSettings["keyAES"]);
byte[] iv =
Encoding.UTF8.GetBytes(ConfigurationManager.AppSettings["IVAES"]);
System.Console.WriteLine(Encrypt_Aes(credit, key, iv));
```

```
private static string Encrypt_Aes(string plainText, byte[] Key, byte[] IV)
        {
            // Check arguments.
            if (plainText == null || plainText.Length <= 0)
                throw new ArgumentNullException("plainText");
            if (Key == null || Key.Length <= 0)
                throw new ArgumentNullException("Key");
            if (IV == null || IV.Length <= 0)
                throw new ArgumentNullException("Key");

            byte[] encrypted;
            // Create an Aes object
            // with the specified key and IV.
            using (Aes aesAlg = Aes.Create())
            {
                aesAlg.Key = Key;
                aesAlg.IV = IV;

                // Create a decryptor to perform the stream transform.
                ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key,
aesAlg.IV);

                // Create the streams used for encryption.
                using (MemoryStream msEncrypt = new MemoryStream())
                {
                    using (CryptoStream csEncrypt = new CryptoStream(msEncrypt,
encryptor, CryptoStreamMode.Write))
                    {
                        using (StreamWriter swEncrypt = new
StreamWriter(csEncrypt))
                        {
                            //Write all data to the stream.
```

```
                    swEncrypt.Write(plainText);
                }
                encrypted = msEncrypt.ToArray();
            }
        }
    }
    // Return the encrypted bytes from the memory stream.
    return Convert.ToBase64String(encrypted);
}

private static string Decrypt_Aes(string encryptedText, byte[] Key, byte[]
IV)
{
    byte[] cipherText = Convert.FromBase64String(encryptedText);
    // Check arguments.
    if (cipherText == null || cipherText.Length <= 0)
        throw new ArgumentNullException("cipherText");
    if (Key == null || Key.Length <= 0)
        throw new ArgumentNullException("Key");
    if (IV == null || IV.Length <= 0)
        throw new ArgumentNullException("Key");

    // Declare the string used to hold
    // the decrypted text.
    string plaintext = null;

    // Create an Aes object
    // with the specified key and IV.
    using (Aes aesAlg = Aes.Create())
    {
        aesAlg.Key = Key;
        aesAlg.IV = IV;
```

```
            // Create a decrytor to perform the stream transform.
            ICryptoTransform decryptor = aesAlg.CreateDecryptor(aesAlg.Key,
aesAlg.IV);


            // Create the streams used for decryption.
            using (MemoryStream msDecrypt = new
MemoryStream(cipherText))
            {
               using (CryptoStream csDecrypt = new CryptoStream(msDecrypt,
decryptor, CryptoStreamMode.Read))
                {
                   using (StreamReader srDecrypt = new
StreamReader(csDecrypt))
                    {


                       // Read the decrypted bytes from the decrypting stream
                       // and place them in a string.
                       plaintext = srDecrypt.ReadToEnd();
                    }
                }
            }
        }
        return plaintext;
    }
```

- Sử dụng:

```
// 1. Lưu trữ scecretKey trong file cấu hình an toàn
// 2. Mã hóa các dữ liệu nhạy cảm, ví dụ credit card, PIN number
// 3. Sử dụng thuật toán mã hóa mạnh (AES), secretKey khó đoán
// 4. Xử lí exception trả về thông báo chung
// 5. Ghi log exception trên server
```

➢ ***SQL***

4.1. Sử dụng mô hình truy vấn prepared statement (parameterized query) hoặc các hình thức tương đương.

- Ví dụ sử dụng mô hình truy vấn tham số trong ADO.Net:

```
string sql = "SELECT * FROM Users WHERE UserName=@username AND Password=@password";
SqlCommand command = new SqlCommand(sql, connection);
command.Parameters.AddWithValue("@username", username);
command.Parameters.AddWithValue("@password", password);
DbDataReader reader = command.ExecuteReader();
```

4.2. Trong 1 số trường hợp không sử dụng được các mô hình ở trên, cần thiết lập danh sách whitelist các đầu vào mong muốn.

- Ví dụ với trường hợp không thể sử dụng mô hình truy vấn tham số là "order by" query:

```
private const string[] orderByWhiteList = new string[] { "name", "age",
    "class"};
public static Boolean isInOrderByWhiteList(string input)
{
    return orderByWhiteList.Contains(input);
}
```

➢ ***NoSQL***

4.3. Không mở service ra ngoài public internet, cài đặt trong môi trường mạng an toàn (trusted environments).

- Cấu hình chỉ mở localhost interface trong trường hợp ứng dụng cùng host với database, tắt các các dịch vụ không cần thiết. Trường hợp, cần kết nối database remote, cấu hình firewall giới hạn ip cho phép kết nối.

- Ví dụ, với mongodb 3.0.4, cấu hình chỉ lắng nghe trên interface 127.0.0.1, tắt http, json, rest interface.

```
net:
  port: 27017
  bindIp: 127.0.0.1
  http:
    enabled: false
    JSONPEnabled: false
    RESTInterfaceEnabled: false
```

4.4. Đối với các hệ NoSQL có hỗ trợ xác thực, cần cấu hình xác thực khi truy cập.

Mặc định các hệ NoSQL tắt tính năng xác thực, cụ thể đối với mongodb 3.0.4, sau khi cài đặt, server chưa có người dùng và cũng không bật xác thực, thực hiện các bước sau để tạo người dùng với các quyền tương ứng và bật tính năng xác thực:

- Tạo người dùng quản trị server

```
use admin
db.createUser(
  {
    user: "administrator",
    pwd: "M@tkhauKh0Do@n",
    roles: [ { role: "userAdminAnyDatabase", db: "admin" } ]
  }
)
```

- Tạo người dùng quản trị cho 1 database (ví dụ DB baseline)

```
use baseline
db.createUser(
  {
    user: "admin_baseline",
    pwd: "M@tkhauKh0Do@n",
    roles: [ { role: "userAdmin", db: "baseline" } ]
  }
)
```

- Tạo người dùng sử dụng DB đó (có quyền thêm, sửa, xóa truy vấn)

```
use baseline
db.createUser(
  {
    user: "user_baseline",
    pwd: "M@tkhauKh0Do@n",
    roles: [ { role: "readWrite", db: "baseline" } ]
  }
```

```
)
```

- Cuối cùng, cấu hình mongodb bật tính năng xác thực và phân quyền

```
security:
    authorization: true
```

- Sử dụng mongo-c#-driver để kết nối đến mongodb

```
string user = "admin";
string database = "test";
char[] password = "M@tkhauKh0Do@n".ToCharArray();
MongoServerSettings settings = new MongoServerSettings();
var credential = MongoCredential.CreateMongoCRCredential(database, user, password);
var settings = new MongoClientSettings
{
    Credentials = new[] { credential }
};
var mongoClient = new MongoClient(settings);
MongoDatabase testDB = mongoClient.getDatabase(database);
```

4.5. Phụ thuộc vào hệ NoSQL sử dụng, sử dụng các api hỗ trợ truy vấn an toàn hoặc thực hiện escape các ký tự đặc biệt khi xây dựng câu truy vấn.

Đối với mongodb, sử dụng api mongo-c#-driver khi thực hiện các thao tác thêm, sửa, xóa, tìm kiếm:

- Thêm document cho collection

```
var collection = database.GetCollection<Entity>("entities");
var entity = new Entity { Name = "Tom" };
collection.Insert(entity);
var id = entity.Id;
```

- Sửa document trong collection

```
var query = Query<Entity>.EQ(e => e.Id, id);
var update = Update<Entity>.Set(e => e.Name, "Harry");
collection.Update(query, update);
```

- Xóa document trong collection

```
var query = Query<Entity>.EQ(e => e.Id, id);
collection.Remove(query);
```

- Tìm kiếm document trong collection. Cách an toàn là sử dụng các api Filters, Sorts, Projections để tạo truy vấn tìm kiếm

```
var query = Query<Entity>.EQ(e => e.Id, id);
var entity = collection.FindOne(query);
```

➢ ***XPath***

4.6. Thiết lập danh sách whitelist các ký tự đầu vào mong muốn, đầu vào nên là tập hợp của chữ cái, chữ số.

```
public static Boolean isValidInput(string input)
    {
       if (input == null)
          return false;
       else
          return Regex.IsMatch(input, "^[a-zA-Z0-9._]+$");
    }
```

4.7. Lập danh sách blacklist các ký tự đặc biệt (( ) = ‘[ ] : , * / và dấu cách), loại bỏ các đầu vào có chứa các ký tự nằm trong blacklist.

```
public static Boolean isInValidInput(string input)
    {
       if (input == null)
          return false;
       string[] blackList = new string[] { "[()='\\[\\]:,*/ ]" };
       return blackList.Contains(input);
    }
```

➢ ***LDAP***

4.1. Thiết lập danh sách whitelist các ký tự đầu vào mong muốn, đầu vào nên là tập hợp của chữ cái, chữ số.

```
public static Boolean isValidInput(string input)
    {
```

```
        if (input == null)
            return false;
        else
            return Regex.IsMatch(input, "^[a-zA-Z0-9._]+$");
    }
```

4.8. Lập danh sách blacklist các ký tự đặc biệt (( ) ; , * | & = và nullbyte), loại bỏ các đầu vào có chứa các ký tự nằm trong blacklist.

```
public static Boolean isInValidInput(string input)
    {
        if (input == null)
            return false;
        string[] blackList = new string[] { "[()='\\[\\]:,*/ ]" };
        return blackList.Contains(input);
    }
```

➢ ***Tương tác với OS***

4.9. Sử dụng các API hỗ trợ việc thực thi câu lệnh hệ thống.

```
public static Boolean checkUseSafeApi()
    {
        string hostname = "10.2.0.30";
        HttpWebRequest request =
(HttpWebRequest)WebRequest.Create(hostname);
        request.Timeout = 15000;
        request.Method = "HEAD";
        try
        {
            using (HttpWebResponse response =
(HttpWebResponse)request.GetResponse())
            {
                return response.StatusCode == HttpStatusCode.OK;
            }
        }
        catch (WebException)
```

```
        {
            return false;
        }
    }
```

4.10. Không truyền trực tiếp dữ liệu người dùng truyền lên tới OS, trong trường hợp bắt buộc cần thiết lập danh sách whitelist các đầu vào mong muốn.

```
public static void processWhitelist()
    {
        string hostname = "google.com && echo VULNERABLE";
        string DOMAIN_NAME_PATTERN = "^((?!-)[A-Za-z0-9-
]{1,63}(?<!-)\\.)+[A-Za-z]{2,6}$";
        string IPADDRESS_PATTERN
              = "^([01]?\\d\\d?|2[0-4]\\d|25[0-5])\\."
              + "([01]?\\d\\d?|2[0-4]\\d|25[0-5])\\."
              + "([01]?\\d\\d?|2[0-4]\\d|25[0-5])\\."
              + "([01]?\\d\\d?|2[0-4]\\d|25[0-5])$";

        if (!Regex.IsMatch(hostname, DOMAIN_NAME_PATTERN) &&
!Regex.IsMatch(hostname, IPADDRESS_PATTERN))
        {
            Console.WriteLine("Hostname is not valid");
            return;
        }
        System.Diagnostics.Process process = new
System.Diagnostics.Process();
        System.Diagnostics.ProcessStartInfo startInfo = new
System.Diagnostics.ProcessStartInfo();
        startInfo.WindowStyle =
System.Diagnostics.ProcessWindowStyle.Hidden;
        startInfo.FileName = "cmd.exe";
        startInfo.Arguments = "/c ping" + hostname;
        process.StartInfo = startInfo;
        process.Start();
```

```
    }
```

➢ ***Tương tác với file***

4.11. Không truyền trực tiếp dữ liệu từ người dùng đến các hàm include file.

4.12. Lập danh sách whitelist các định dạng file được phép upload.

.Net hỗ trợ lọc file upload bằng cách thiết lập trong web.config như sau:

```
<configuration>
    <system.webServer>
        <security>
            <requestFiltering>
                <fileExtensions applyToWebDAV="false">
                    <add fileExtension=".ashx" allowed="false" />
                </fileExtensions>
                <!-- maxAllowedContentLength is in bytes -->
                <requestLimits maxAllowedContentLength="5242880"/> <!--
    5MB -->
            </requestFiltering>
        </security>
    </system.webServer>
</configuration>
```

4.13. Validate file hợp lệ bằng cách kiểm tra đồng thời file header, phần mở rộng của file và nội dung file.

Ví dụ upload 1 file ảnh lên server:

```
foreach (string upload in Request.Files)
        {
            var allowedExtensions = new[] { ".png", ".bmp", ".jpeg" };
            if (Request.Files[upload].ContentLength == 0) continue;
            string path = Path.Combine(@"D:\MyUploadedFiles");
            var extension =
Path.GetExtension(Request.Files[upload].FileName);
            if (!allowedExtensions.Contains(extension))
            {
                return Json(new { Type = "Invalid Extension" });
```

```
            }
            string filename =
Path.GetFileName(Request.Files[upload].FileName);
            Request.Files[upload].SaveAs(Path.Combine(path,
WebApp.Utils.StringUtils.getSafeFilename(filename)));
            UploadFilesResult file = new UploadFilesResult();
            file.FilePath = @"D:\MyUploadedFiles" + filename;
            file.FileName = filename;
            FileRepositories.CreateFile(file);
         }
         return Json(new { Type = "SUCCESS" });
private static String getSafeFileName(String input)
  {
    StringBuilder sb = new StringBuilder();
    for(int i=0; i < input.Length; i++)
    {
      char c = input[i];
      if(c!='/' && c!='\\' && c!=0)
      {
        sb.Append(c);
      }
    }
    return sb.ToString();
  }
```

4.14. Với các trường hợp không bắt buộc thì không lưu file upload trong thư mục web, bỏ quyền thực thi trên thư mục upload.

4.15. Khi cần refer tới các file tồn tại trên hệ thống cần thiết lập danh sách whitelist đầu vào mong muốn hoặc gán các giá trị định danh tương ứng cho các file thay vì truyền tên file.

4.16. Không trả về đường dẫn tuyệt đối của file.

4.17. Tất cả dữ liệu, tài nguyên hệ thống (báo cáo, file upload, file cấu hình...) không được lưu trong thư mục cho phép truy cập trực tiếp không qua xác thực.

- ***Xử lý back-end HTTP request***

4.18. Khi tạo http request phía server, các tham số GET, POST cho request đó tránh tạo từ dữ liệu phía người dùng, hoặc phải được kiểm tra cẩn thận để chống ghi đè các tham số khác.

➢ **Tương tác với XML**

4.19. Tắt tính năng external entity resolve và remote doctype retrival của xml parser khi đọc dữ liệu xml.

- ***.Net 3.5:***

```
MemoryStream stream = new
MemoryStream(Encoding.Default.GetBytes(xml));
XmlTextReader reader = new XmlTextReader(stream);
reader.ProhibitDtd = true;

hoặc

XmlReaderSettings settings = new XmlReaderSettings();
settings.ProhibitDtd = true;
XmlReader reader = XmlReader.Create(stream, settings);
```

- ***.Net 4 & 4.5:***

```
MemoryStream stream = new
MemoryStream(Encoding.Default.GetBytes(xml));
XmlReaderSettings settings = new XmlReaderSettings();
settings.DtdProcessing = DtdProcessing.Prohibit;
XmlReader reader = XmlReader.Create(stream, settings);
```

4.20. Kiểm tra dữ liệu người dùng, encode các kí tự đặc biệt (<>/) khi tạo dữ liệu xml.

5. Kiểm soát dữ liệu đầu vào

5.1. Việc kiểm tra dữ liệu đầu vào phải được thực hiện phía server.

5.2. Thực hiện việc kiểm tra dữ liệu từ tất cả các nguồn dữ liệu có tương tác với người dùng (Các tham số lấy từ GET/POST request, HTTP Headers, dữ liệu lấy từ DB, dữ liệu từ file upload,…).

5.3. Xác định rõ chuẩn định dạng encode của dữ liệu đầu vào, thực hiện validate dữ liệu sau khi đã decode đầu vào về 1 định dạng chuẩn và nhất quán.

5.4. Validate kiểu dữ liệu, phạm vi, độ dài dữ liệu và định dạng dữ liệu.

5.5. Ví dụ một số kiểu validator được hỗ trợ bởi thư viện opensymphony.xwork2 như sau:

```
private static string ValidateUsername(string username)
{
   if (username == null || username.Equals(""))
      return "Name must be required";

   if (!Regex.IsMatch(username, "^(?=.{6,30}$)"))
      return "Name length must be between 6 and 30";

   if (!Regex.IsMatch(username, "^[a-zA-Z0-9_]+$"))
      return "Name contain only letter, number, _";

   return "OK";
}

private static string ValidateAge(int age)
{
   if (age < 0 | age > 60)
      return "Age must from 0 to 60";
   else
      return "OK";
}

private static string ValidateDate(DateTime date)
{
   if (date == null)
      return "notOK";

   DateTime min = new DateTime(1995, 01, 01);
   DateTime max = new DateTime(2015, 12, 31);
```

```
    if (date.CompareTo(min) == -1 | date.CompareTo(max) == 1)
        return "Date must in range 01/01/1955 to 31/12/2015";

    return "OK";
}

private static string ValidateEmail(string email)
{
    if (email == null || email.Equals(""))
        return "Email is required";

    if (!Regex.IsMatch(temp, "^[a-zA-Z0-9._-]{1,64}@[A-Za-z0-
9]{2,64}(\\.[A-Za-z0-9]{2,64})*(\\.[A-Za-z]{2,4})$"))
        return "Email format not correct";

    return "OK";
}
```

5.6. Nếu dữ liệu đầu vào bắt buộc là các ký tự đặc biệt, cần thiết lập danh sách whitelist các ký tự đầu vào mong muốn.

6. Kiểm soát dữ liệu đầu ra

6.1. Phải chỉ rõ character encoding cho dữ liệu đầu ra: Thực hiện tương tự mục 5.3.

6.2. Response body phải được encode theo ngữ cảnh sử dụng. Một số trường hợp phổ biến:

- Đầu ra là html, thực hiện html encode các kí tự đặc biệt (<>’”&) từ các nguồn dữ liệu không an toàn (Các tham số lấy từ GET/POST request, HTTP Headers, dữ liệu lấy từ DB, dữ liệu từ file upload,… có thể điều khiển được bởi người dùng).

```
<label id="label1" runat="server"></label>

Cách 1: Dùng HttpUtility.HtmlEncode
label1.InnerHtml = HttpUtility.HtmlEncode(str);

Cách 2: Dùng InnerText
```

```
label1.InnerText = str;
```

- Đầu ra là json, thực hiện encode dữ liệu trả về dạng object, không trả về dạng mảng.

6.3. Response header: lọc bỏ các kí tự đặc biệt (\n, \r) do dữ liệu người dùng truyền vào.

```
// remove control character [\x00-\x1F\x7F]
header = header.replaceAll("\\p{Cntrl}", "");
```

6.4. Cookie trả về cần giới hạn tối thiểu nhất các thuộc tính (domain, path, httponly, expire, secure). Tránh lưu trữ các dữ liệu nhạy cảm trên cookie, nếu cần lưu trữ các dữ liệu nhạy cảm thì phải thực hiện mã hóa các dữ liệu này với thuật toán đối xứng mạnh và key chỉ được lưu trên server.

```
HttpCookie cookie = new HttpCookie("ASP.NET_SESSIONID",
cookieValue);
/* 1. Giới hạn thuộc tính của cookie */

// ví dụ cookie cookieOnAdminPage để nhớ đăng nhập trên trang /admin/
    cookie.HttpOnly = true;
    cookie.Secure = true;   // Chỉ dùng nếu có sử dụng Https
    cookie.Path = "/admin/";
    cookie.Value = cookieValue;
cookie.Expires = new DateTime(2015, 12, 20);

/* Mã hóa cookie */
// Thực hiện tương tự mục 4. Tương tác với backend => Mã hóa các dữ
liệu nhạy cảm trước khi lưu trữ
```

6.5. Hạn chế việc chuyển hướng, chuyển tiếp đến các URI khác. Nếu ứng dụng có chức năng này cần phải lập danh sách whitelist các URL được phép thực hiện chuyển hướng, chuyển tiếp.

```
private static string[] allowedURL = { "voffice.abc.vn",
"thongtinnhansu.abc.vn", "abc.vn" };

public static Boolean isAllowedURL(string url){
    return allowedURL.Contains(url .ToLower().Trim());
```

```
}
```

7. Kiểm soát ngoại lệ và ghi log ứng dụng

7.1. Xử lý các ngoại lệ bằng try-catch và trả về các thông báo lỗi chung đã custom, thông báo lỗi trả về không được chứa các thông tin nhạy cảm của người dùng, hệ thống...

```
<configuration>
   <system.web>
      <customErrors defaultRedirect="myCustomErrorPage.aspx"
         mode="RemoteOnly">
      <error statusCode="500"
         redirect="InternalError.htm"/>
      </customErrors>
   </system.web>
</configuration>
```

7.2. Các thông tin lỗi, ngoại lệ này phải được log lại để phục vụ bảo trì, xác định nguyên nhân lỗi ứng dụng.

Sử dụng thư viện log4net để ghi log ứng dụng.

7.3. File log phải được đặt tại thư mục an toàn ngoài thư mục web.

7.4. Không log lại các dữ liệu nhạy cảm (thông tin người dùng, session id, thông tin hệ thống).

Mục 7.3 và 7.4 thực hiện cấu hình log4net tại file web.config như sau:

```
<log4net>
   <appender name="LogFileAppender"
type="log4net.Appender.RollingFileAppender">
      <param name="File" value="D:\logs\abc\wflog.log"/>
      <param name="AppendToFile" value="true"/>
      <rollingStyle value="Size"/>
      <maxSizeRollBackups value="10"/>
      <maximumFileSize value="3MB"/>
      <staticLogFileName value="true"/>
      <layout type="log4net.Layout.PatternLayout">
      <param name="ConversionPattern" value="%d{HH:mm:ss.SSS} %t
%C{1} %-5p %n%l%n%m%n%n"/>
```

```
        </layout>
    </appender>

<!-- Ví dụ cấu hình logger cho package com.abc -->
    <logger name="CentralCMS">
        <level value="DEBUG"/>
    </logger>

    <root>
        <level value="Debug"/>
        <appender-ref ref="LogFileAppender"/>
    </root>
</log4net>
```

7.5. Giới hạn người dùng cho phép truy cập file log.

8. Sử dụng framework, lib (third-party components)

8.1. Loại các thành phần, lib không cần thiết.

8.2. Sử dụng phiên bản mới nhất của framework tại thời điểm phát triển ứng dụng.

8.3. Thường xuyên cập nhật các bản vá lỗi cho framework.

8.4. Tắt chế độ development của framework khi triển khai ứng dụng thực tế.

Cấu hình trong file web.config:

```
<compilation debug="false" />
```

9. Xử lý business logic

Xử lý business logic phụ vào từng ứng dụng nhưng lưu ý:

9.1. Lập trình viên phải nắm rõ được toàn bộ luồng nghiệp vụ của ứng dụng, phải xây dựng các cây testcase cho từng nghiệp vụ để tránh bỏ sót các trường hợp có thể xảy ra.

9.2. Các chức năng quan trọng (ví dụ chuyển khoản ngân hàng), sử dụng lock hoặc các hình thức tương đương để tránh lỗi race condition.

Phụ lục 03.
HƯỚNG DẪN LẬP TRÌNH AN TOÀN SỬ DỤNG ỨNG DỤNG C/C++

1. Biên dịch an toàn

Chú ý: Các yêu cầu thiết lập trình biên dịch dưới đây chỉ áp dụng khi trình biên dịch cho hệ điều hành, vi xử lý hoặc vi điều khiển có hỗ trợ tính năng tương ứng.

1.1. Biên dịch với tùy chọn chống ghi đè bộ đệm (TC.LTAT.CCPP.1.1; Bắt buộc)

1.1.1. Nguy cơ

Lỗi hay gặp nhất trong lập trình C/C++ là lỗi buffer overflow, khi đó nếu chương trình không được biên dịch với tùy chọn chống ghi đè bộ đệm thì hacker có thể chèn mã lệnh ghi đè bộ đệm dễ dàng khai thác lỗi buffer overflow thực thi mã lệnh đó.

1.1.2. Giải pháp

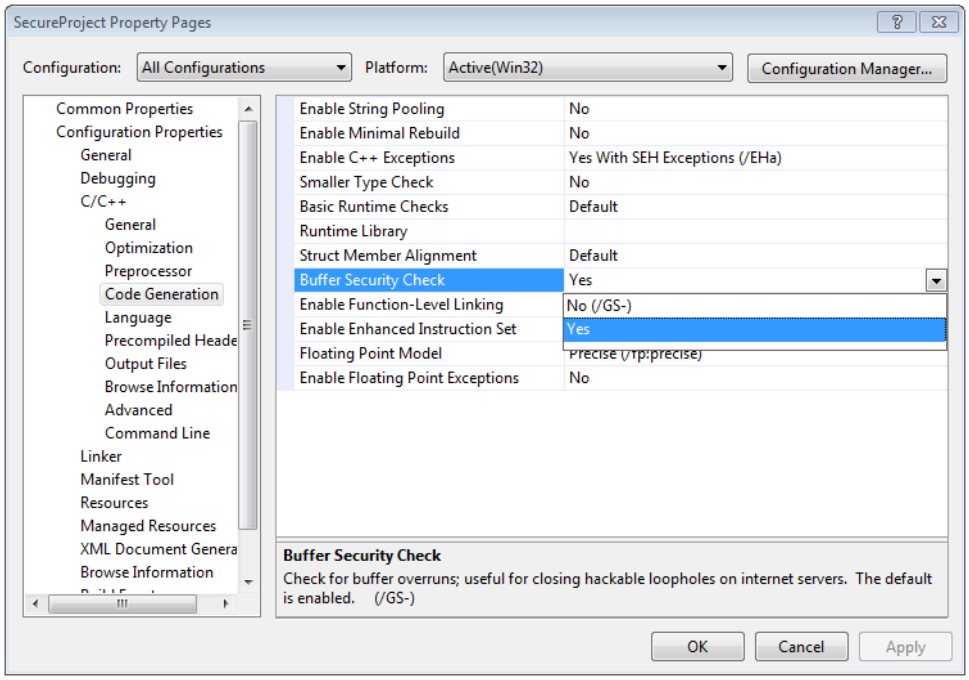
- Biên dịch dùng Visual Studio: Bật kiểm tra bộ đệm (/GS): default từ Visual Studio 2003.

- Có 2 cách:

  - Sử dụng hướng dẫn biên dịch trong code:

    #pragma strict_gs_check(on)

  - Cấu hình trên Editor: Trong cửa sổ Properties của Project, chọn C++ Code generation, bật Buffer Security Check:



- Biên dịch dùng gcc: Sử dụng cờ -fstack-protector-all khi biên dịch.

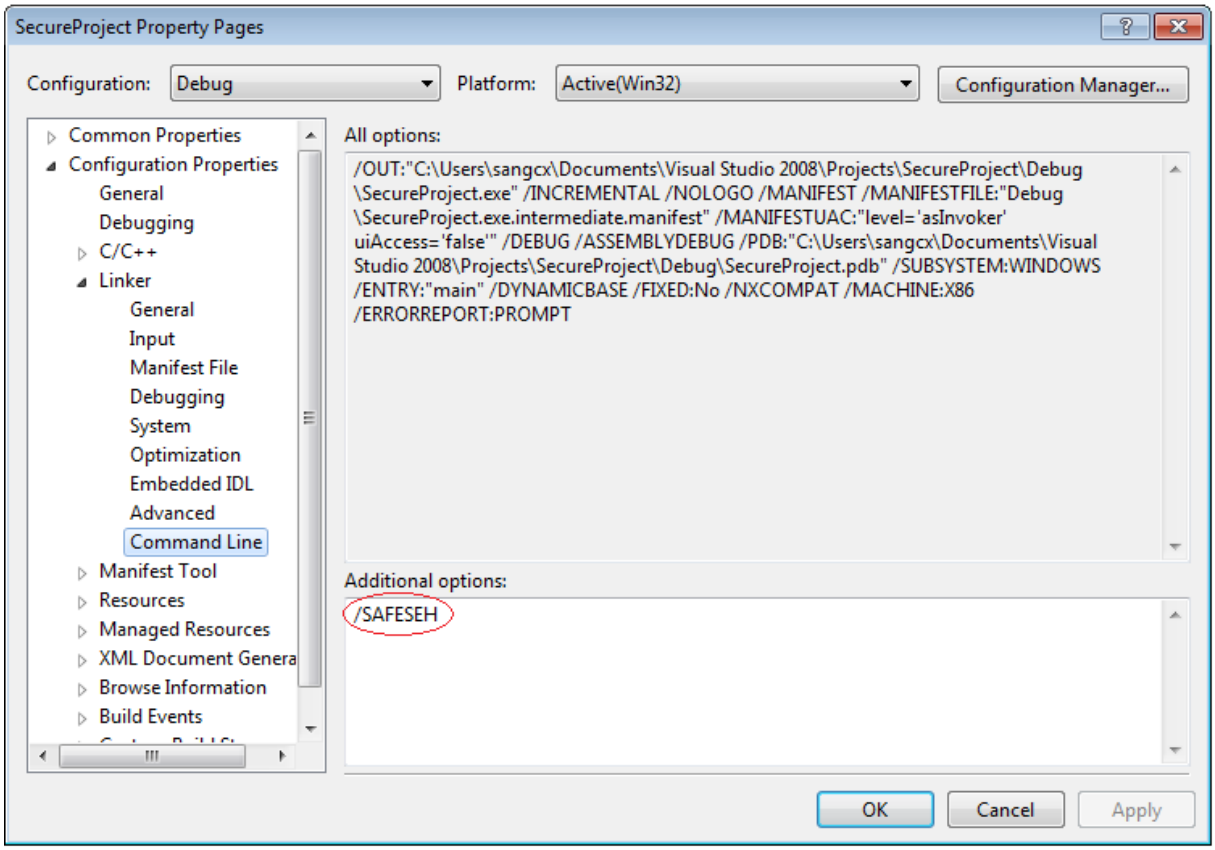
1.2. Biên dịch với tùy chọn chống khai thác qua SEH (Struct Exception Handling) (chỉ có trên Windows) (TC.LTAT.CCPP.1.2; Bắt buộc)

1.2.1. Nguy cơ

- Một trong những cách thức tấn công khai thác lỗi Buffer Overflow là ghi đè cấu trúc SEH (là 1 cấu trúc do Microsoft đưa ra nhằm xử lý các ngoại lệ), trong đó hacker lợi dụng cách Windows xử lý các cấu trúc SEH để chèn mã lệnh thực thi. Chương trình không biên dịch với tùy chọn /SafeSEH có thể bị khai thác kiểu này khi có lỗi buffer overflow.

1.2.2. Giải pháp

- Trong cửa sổ Properties của Project, chọn Linker Command Line, trong ô Additional options, điền vào /SafeSEH:



1.3. Biên dịch với tùy chọn DEP không cho chạy mã lệnh trên vùng data (TC.LTAT.CCPP.1.3; Bắt buộc)

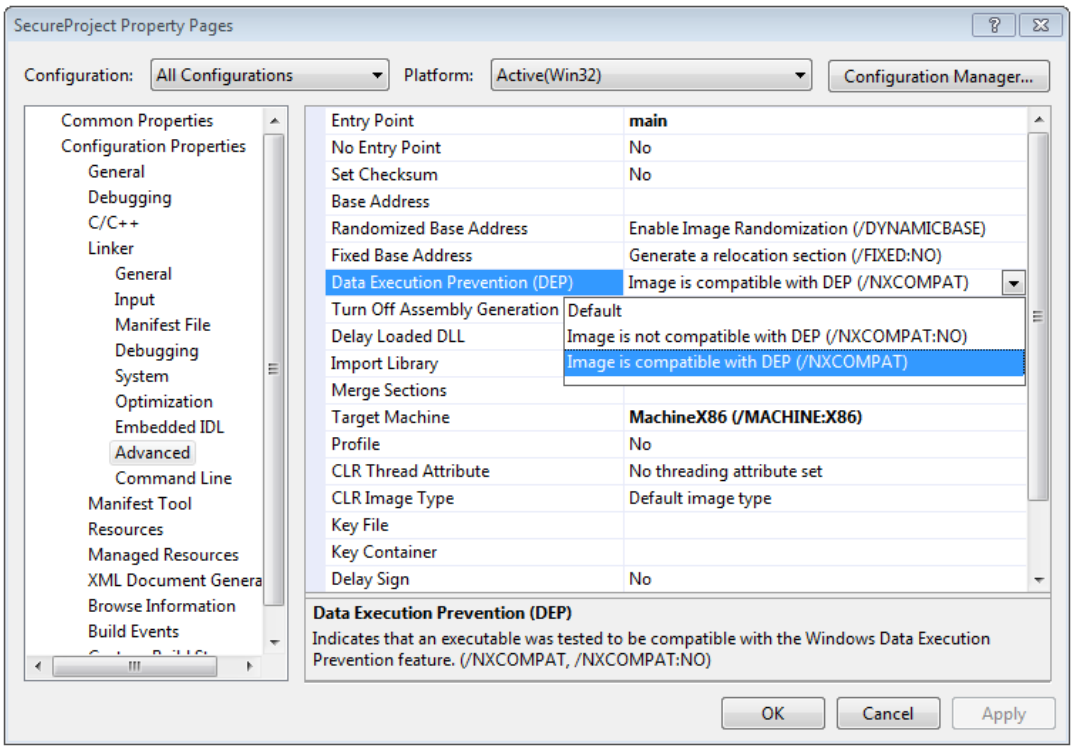
1.3.1. Nguy cơ

- DEP (Data Execution Prevention) là một cơ chế trong kiến trúc vi xử lý trong đó đánh dấu vùng nhớ nào là dữ liệu thì nếu con trỏ lệnh chỉ vào vùng dữ liệu thì sẽ phát sinh cảnh báo lỗi. Tuy nhiên với chương trình không biên dịch với tùy chọn DEP thì hệ điều hành sẽ thực thi chương trình mà không sử dụng cơ chế đó. Điều này làm cho chương trình dễ bị tổn thương hơn với các kiểu tấn công vào bộ nhớ (như buffer overflow, use after free, integer overflows,...) trong đó thông thường hacker sẽ tìm cách chuyển con trỏ lệnh về 1 vùng nhớ dữ liệu mà hacker thay đổi được.

1.3.2. Giải pháp

- Biên dịch dùng Visual Studio (có từ Visual Studio 2005): Bật tùy chọn không cho chạy mã lệnh trên vùng data DEP - Data Execution Prevention: Image is compatible with DEP (/NXCOMBAT).

- Trong cửa sổ Properties của Project, chọn Linker Advanced, trong ô Data Execution Prevention (DEP), chọn Image is compatible with DEP:



- Biên dịch dùng gcc cho ứng dụng trên Windows: -WI,--nxcompat.

1.4. Biên dịch chương trình với tùy chọn cho phép nạp lên bộ nhớ ở địa chỉ ngẫu nhiên (TC.LTAT.CCPP.1.4; Bắt buộc)

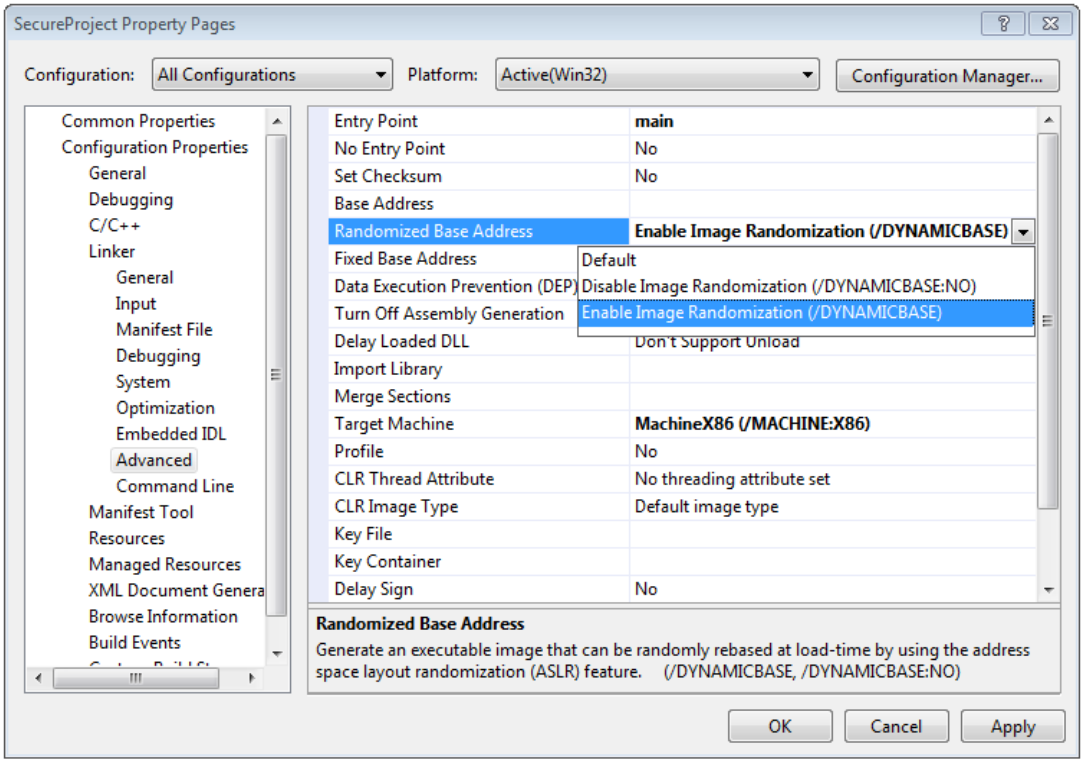
1.4.1. Nguy cơ

- Khi hacker khai thác các lỗi tấn công vào bộ nhớ, một việc hacker thường phải làm là xác định vị trí gốc chương trình nạp lên. Nếu chương trình biên dịch không có tùy chọn cho phép nạp lên bộ nhớ ở địa chỉ ngẫu nhiên thì khi đó hacker có thể xác định được ngay địa chỉ đó, tùy thuộc vào phiên bản, loại hệ điều hành.

1.4.2. Giải pháp

- Biên dịch dùng Visual Studio (có từ Visual Studio 2005): Bật tùy chọn Randomized Base Adress (/Dynamic Base).

- Trong cửa sổ Properties của Project, chọn Linker Advanced, trong ô Randomized Base Address (DEP), chọn Enable Image Randomization (/DYNAMICBASE):



- Biên dịch dùng gcc: Sử dụng cờ -fPIE khi biên dịch.

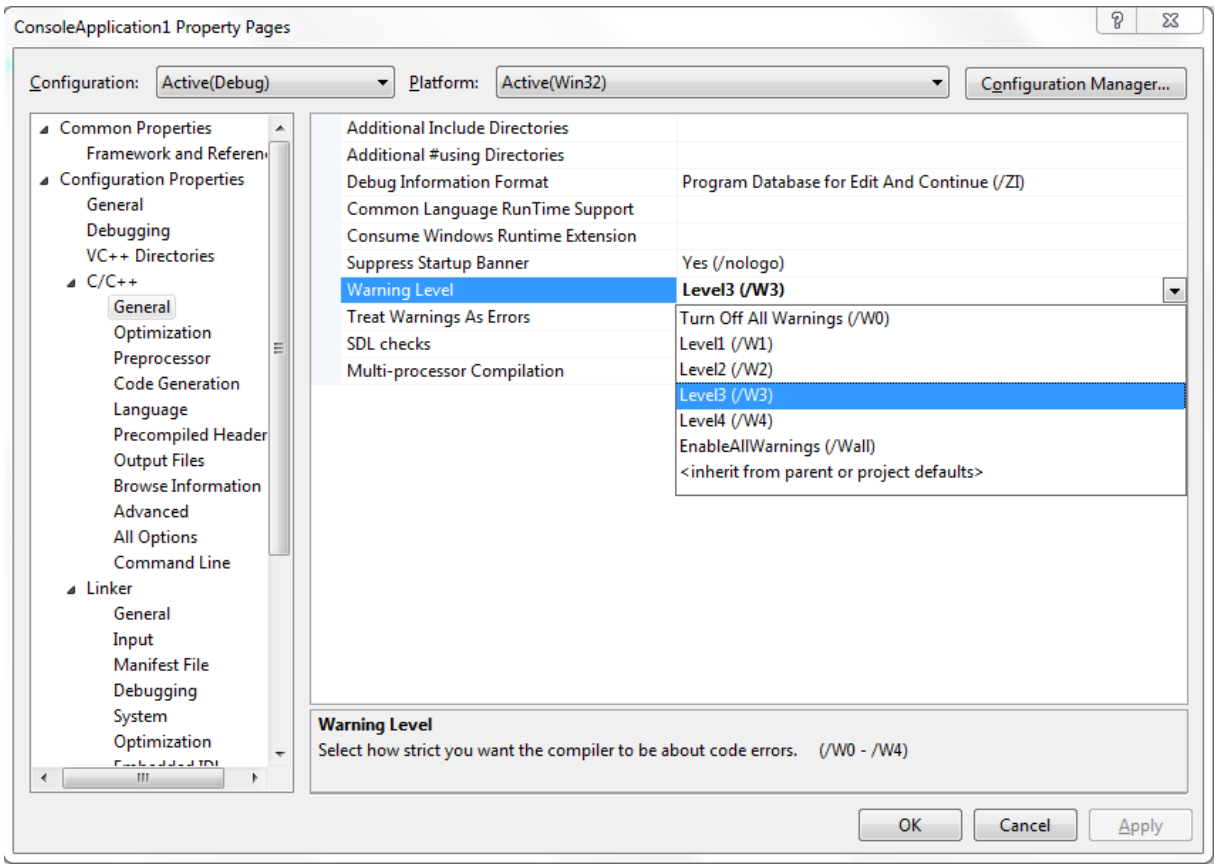
1.5. Bật cảnh báo khi biên dịch (TC.LTAT.CCPP.1.5; Bắt buộc)

1.5.1. Nguy cơ

- Khi biên dịch, thông thường công cụ biên dịch đã hỗ trợ khá nhiều tính năng cảnh báo các dạng lỗi cơ bản dễ gặp phải. Nếu tắt tùy chọn cảnh báo khi biên dịch hoặc tùy chọn mức thấp thì có thể lập trình viên đã bỏ qua những lỗi cơ bản.

1.5.2. Giải pháp

- Biên dịch dùng Visual Studio: Đặt Warning level ở mức: /W3.



- Biên dịch dùng gcc: Sử dụng cờ -Wall.

2. Bảo vệ ứng dụng an toàn khỏi các lỗi bộ nhớ

2.1. Lỗi tràn bộ đệm (buffer overflow) (TC.LTAT.CCPP.2.1; Bắt buộc)

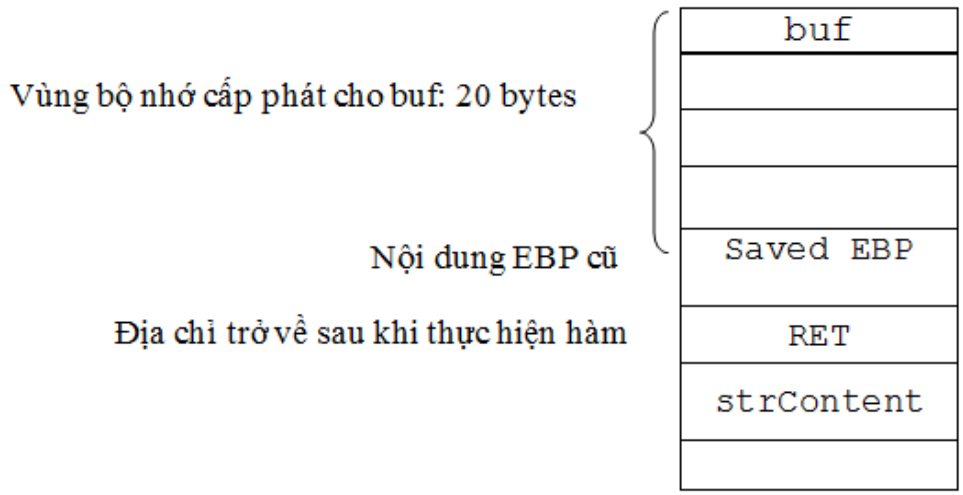
2.1.1. Mô tả lỗi

- Buffer là một vùng nhớ được cấp phát trên bộ nhớ trong quá trình thực thi ứng dụng.

- Lỗ hổng tràn bộ đệm (Buffer overflow - Bof) là lỗ hổng xảy ra khi ghi khối dữ liệu lớn hơn kích thước của vùng nhớ buffer được cấp phát. Ví dụ:

```
void OverFlow(char *strContent)
{
        char buf[20];
        strcpy(buf, strContent);
        return;
}
```

Hình ảnh của stack khi gọi ứng dụng gọi hàm Overflow:



- Khi kích thước của strContent lớn hơn kích thước được cấp phát của buf, nội dung của strContent sẽ ghi đè lên các vùng địa chỉ khác.

2.1.2. Nguy cơ

- Khi lỗi tràn bộ đệm xảy ra nội dung của các vùng nhớ bị ghi đè dẫn tới chương trình hoạt động không chính xác hoặc bị đổ vỡ (crash).

- Nguy hiểm hơn bằng cách khai thác một cách có chủ đích, hacker có thể chèn mã lệnh vào một chương trình có nguy cơ tràn bộ đệm và thực thi mã lệnh đó. Ví dụ: bằng cách ghi đè địa chỉ trả về của hàm.

2.1.3. Giải pháp

- Kiểm soát kích thước của dữ liệu truyền vào:
    - Mỗi khi sử dụng cần kiểm tra kích thước bộ đệm để đảm bảo việc truy nhập không vượt ra ngoài phạm vi bộ đệm.

```
void NoneOverFlow(const char *strContent)
{
	char buf[20];
	if (strlen(strContent)< 20)
	{
		strcpy(buf, strContent);
		return;
	}
	else
	{
```

```
            // do something
        }
}
```

```
int CalculateBufferValue(LPBYTE buffer, int len, int index)
{
        if (buffer == NULL ||           // Địa chỉ bộ đệm không hợp lệ
                len <= 0 ||             // Hoặc kích thước bộ đệm không đúng
                index < 0 || index >= len) // Hoặc truy xuất ra ngoài bộ đệm
        {
                return ERROR_CODE;
        }
        …
        result += buffer[index];
        …
}
```

- Khi thiết kế hàm có thao tác với bộ nhớ, nên có tham số chỉ định kích thước tối đa của bộ nhớ.

Nên	**Không nên**

void Scan(char *buffer, int maxLen)
{
strncpy(buffer, name,
maxLen – 1);
buffer[maxLen – 1] = 0;
…
}
	void Scan(char *buffer)
	{
	strcpy(buffer, name);
	
	…
	}

- Sử dụng các hàm thay thế an toàn:

```
char buffer[256];
```

```
strncpy(buffer, filePath, 255); // Giới hạn kích thước tối đa copy vào bộ đệm
buffer[255] = 0; // Đảm bảo string có kết thúc hợp lệ
```

Hoặc:

```
char buf[20];
strcpy_s(buf, 20, strContent);
```

- Danh sách các hàm thay thế an toàn tham khảo **Mục 6. Danh sách các hàm thay thế trong lập trình an toàn sử dụng ứng dụng C/C++.**

2.2. Lỗi tràn số nguyên (integer overflow) (TC.LTAT.CCPP.2.2; Bắt buộc)

2.2.1. Mô tả lỗi

- Là lỗi xảy ra do giá trị của biến vượt quá khoảng giá trị của kiểu dữ liệu tương ứng. Ví dụ:

```
        char i;
        i = SCHAR_MAX; // 127
        i++;
or
        unsigned int j;
        j = UINT_MAX; //65535
        j++;
```

2.2.2. Nguy cơ

- Lỗi tràn số nguyên xảy ra làm cho chương trình hoạt động không đúng, tùy vào từng trường hợp cụ thể lỗi số nguyên có thể dẫn tới nhiều nguy cơ khác.

- VD: Lỗi tràn số nguyên dẫn tới nguy cơ bị lỗ hổng buffer overflow:

```
int main(int argc, char *const *argv)
{
        size_t total;
        total = strlen(argv[1])+strlen(argv[2])+1;
        char *buff = (char *)malloc(total);
        strcpy(buff, argv[1]);
```

```
        strcat(buff, argv[2]);
        return 0;
}
```

2.2.3. Giải pháp

- Kiểm soát các giá trị mà các biến có thể nhận được.

```
int main(int argc, char *const *argv)
{
        size_t total;
        total = strlen(argv[1])+ strlen(argv[2]) + 1;
        if (total > strlen(argv[1]))
        {
                char *buff = (char *)malloc(total);
                strcpy_s(buff, total, argv[1]);
                strcat_s(buff, total, argv[2]);
        }
        else
        {
                // integer overflow
        }
        return 0;
}
```

- Sử dụng kiểu dữ liệu phù hợp để tránh trường hợp tràn số. VD: hàm strlen trả về giá trị có kiểu dữ liệu size_t vì vậy ta nên sử dụng kiểu size_t cho biến total. Nếu total có kiểu dữ liệu unsigned char, strlen(argv[1]) = 254, strlen(argv[2]) = 257. Khi đó, total = 254 + 257 = 255 dẫn đến tràn buffer khi ta chép thêm xâu argv[2] vào buffer (trong trường hợp sử dụng hàm strcat thay vì strcat_s).

- Sử dụng kiểu giá trị lớn hơn trong các phép toán. VD:

```
short a;
short b;
unsigned long sum;          // NOT USE: unsigned int sum
sum = a+b;
```

2.3. Lỗi sử dụng định dạng xâu (format string) (TC.LTAT.CCPP.2.3; Bắt buộc)

2.3.1. Mô tả lỗi

- Format string là họ các hàm vào ra dữ liệu có truyền vào tham số là định dạng của kiểu dữ liệu (Format token: %d, %x, %s, %n,…).

- VD: printf, fprintf, sprint, scanf,…

- Các hàm format string có thể làm việc được với nhiều kiểu truyền tham số khác nhau:

  - Kiểu 1: prinf("%s", msg);
  - Kiểu 2: prinf(msg);

- Điểm quan trọng là các trình biên dịch không phân biệt rõ ràng 2 cách sử dụng trên và nếu như trong cách sử dụng thứ 2 nội dung tham số truyền vào (biến msg) có các ký tự format token (%d, %x, %s, %n,…) thì ứng dụng sẽ thực hiện không chính xác dẫn tới các nguy cơ về ATTT.

2.3.2. Nguy cơ

Việc khai thác lỗ hổng format string có thể dẫn tới:

- Denial of service: bằng cách truyền vào hàng loạt các ký tự format token (VD: *%s%s%s%s*…) ứng dụng sẽ có nguy cơ bị crash vì tham chiếu đến các vùng nhớ trái phép hoặc không tồn tại.

- Đọc được nội dung của một địa chỉ bất kỳ trong bộ nhớ: bằng cách truyền vào nội dung có chứa địa chỉ cùng với các format token một cách có chủ ý.

- Thực thi các đoạn mã độc: bằng cách sử dụng format token %n có thể ghi đè địa chỉ trả về của hàm dẫn tới vùng địa chỉ chứa đoạn mã độc được truyền vào.

2.3.3. Giải pháp

Tránh lỗ hổng format string bằng cách:

- Truyền dữ liệu đầu vào đầy đủ các format token (kiểu 1), không sử dụng các theo kiểu 2.

- Sử dụng các hàm làm việc với string thay thế an toàn (tham khảo danh sách hàm thay thế an toàn trong **Mục 6. Danh sách các hàm thay thế trong lập trình an toàn sử dụng ứng dụng C/C++.**

- Thận trọng khi sử dụng format token %n, đảm bảo truyền vào tham số nhận số lượng ký tự đã xuất ra.

- VD: prinf_s() thay thế cho prinf(),
  sprintf_s() thay thế cho sprintf()

2.4. Lỗi sử dụng vùng nhớ sau khi giải phóng (use after free hoặc using freed memory) (TC.LTAT.CCPP.2.4; Bắt buộc)

2.4.1. Mô tả lỗi

- Lỗi use after free xảy ra khi chương trình tiếp tục sử dụng một con trỏ đến vùng nhớ sau khi đã giải phóng nó. VD:

```
        char* ptr = (char*)malloc (SIZE);
    ...
    if (err) {
        abrt = 1;
        free(ptr);
    }
    ...
    if (abrt) {
        logError("operation aborted before commit", ptr);
    }
```

2.4.2. Nguy cơ

- Thông thường lỗi sẽ dẫn đến crash chương trình (khiến chương trình dừng chạy, báo lỗi). Lỗi use after free đôi khi không có thể hiện gì đặc biệt, chỉ dẫn đến chương trình chạy không đúng.

- Hacker có thể lợi dụng lỗi này để để định vị lại bộ nhớ gây ra các dạng tấn công tràn bộ đệm.

2.4.3. Giải pháp

Lập trình xử lý với bộ nhớ theo cách an toàn, tập thói quen lập trình tốt khi cấp phát, xử lý bộ nhớ. Tham khảo các cách xử lý bộ nhớ an toàn sau đây:

- **Khởi tạo bộ nhớ**:
    - Không sử dụng con trỏ tới bộ nhớ chưa được khởi tạo. Trước khi sử dụng bộ nhớ phải kiểm tra địa chỉ bộ nhớ có hợp lệ không.

Nên	**Không nên**

LPBYTE buffer = NULL;
 	
// Khởi tạo bộ nhớ
…
 	
if (buffer != NULL)
{
buffer[0] == ‘A’;
}
	LPBYTE buffer;
	
	// Khởi tạo bộ nhớ
	…
	
	buffer[0] == ‘A’;

- Cấp phát bộ nhớ:

- Mỗi khi cấp phát bộ nhớ, phải kiểm tra xem bộ nhớ có được cấp phát thành công hay không:

Nên	Không nên

char *buffer =
(char*)malloc(MAX_PATH);
if (buffer == NULL)
{
// Không c*ấp phát được bộ nhớ*
return;
}
 	
buffer[0] = 'A';
	char *buffer =
	(char*)malloc(MAX_PATH);
	
	buffer[0] = 'A';

- Không được phép giả sử bộ nhớ sau khi cấp phát đã được khởi tạo:

Nên	Không nên

char *buffer =
(char*)malloc(MAX_PATH);
if (buffer == NULL)
{
// Không c*ấp phát được bộ nhớ*
return;
}
 	
// Khởi tạo bộ nhớ
memset(buffer, 0, MAX_PATH * sizeof(char));
 	
// Truy cập bộ nhớ đã khởi tạo
char ch = buffer[0];
	char *buffer =
	(char*)malloc(MAX_PATH);
	if (buffer == NULL)
	{
	// Không c*ấp phát được*
	return;
	}
	
	// Truy cập bộ nhớ chưa khởi tạo
	char ch = buffer[0];

- Giải phóng bộ nhớ:

- Luôn giải phóng bộ nhớ động sau khi sử dụng xong. Sau khi giải phóng, đưa địa chỉ con trỏ về NULL.

```
char *buffer = (char*)malloc(MAX_PATH);
…
if (!CheckBuffer(buffer))
{
	// Giải phóng bộ nhớ sau khi sử dụng
	free(buffer);
	buffer = NULL;
}

…
// Kiểm tra địa chỉ bộ nhớ có hợp lệ hay không trước khi sử dụng
if (buffer)
{
	…
}
```

- Kiểm tra kích thước bộ nhớ:

- Mỗi khi sử dụng cần kiểm tra kích thước bộ đệm để đảm bảo việc truy nhập không vượt ra ngoài phạm vi bộ đệm.

```
int CalculateBufferValue(LPBYTE buffer, int len, int index)
{
	if (buffer == NULL ||		// Địa chỉ bộ đệm không hợp lệ
		len <= 0 ||		// Hoặc kích thước bộ đệm không đúng
		index < 0 || index >= len) // Hoặc truy suất ra ngoài bộ đệm
	{
		return ERROR_CODE;
	}
	…
	result += buffer[index];
	…
```

```
}
```

- Khi thiết kế hàm có thao tác với bộ nhớ, nên có tham số chỉ định kích thước tối đa của bộ nhớ.

Nên	Không nên

void Scan(char *buffer, int maxLen)
{
strncpy(buffer, name,
maxLen – 1);
buffer[maxLen – 1] = 0;
…
}
	void Scan(char *buffer)
	{
	strcpy(buffer, name);
	
	…
	}

- Giới hạn quyền truy cập bộ nhớ:

- Các bộ đệm không cho phép ghi nên được khai báo bằng từ khóa const để tránh các hàm, phương thức khác ghi vào bộ đệm.

```
bool ScanFile(const char *fullPath)
{
    // Khai báo fullPath là const
    // Các thao tác trong hàm này không thể thay đổi nội dung fullPath
}
…

// Gọi hàm ScanFile, trong hàm này bộ đệm filePath không thể bị thay đổi
ScanFile(filePath);
```

- Sử dụng các hàm xử lý bộ nhớ thay thế an toàn (tham khảo danh sách hàm thay thế an toàn trong **Mục 6. Danh sách các hàm thay thế trong lập trình an toàn sử dụng ứng dụng C/C++.**).

3. Truy nhập an toàn với các đối tượng (giá trị biến, file, thư mục, event, mutex, registry value,...)

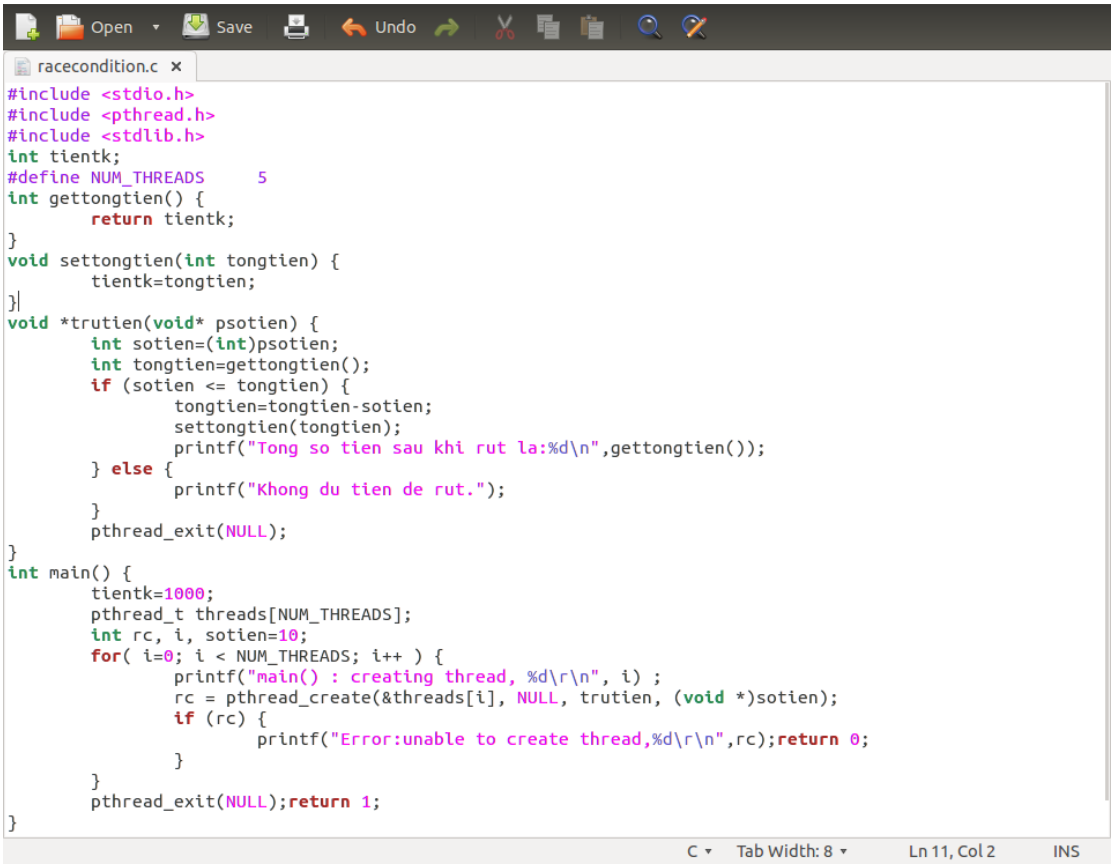
3.1. Tránh lỗi điều kiện tranh chấp (Race-condition) (TC.LTAT.CCPP.3.1; Bắt buộc)

3.1.1. Mô tả lỗi

- Là lỗi xảy ra khi có 2 hay nhiều tiến trình, luồng chạy đồng thời cùng thao tác đến tài nguyên dùng chung và kết quả phụ thuộc vào thứ tự và thời gian thực hiện các tiến trình dẫn đến kết quả xử lý sai, hoặc không đoán được của hệ thống.

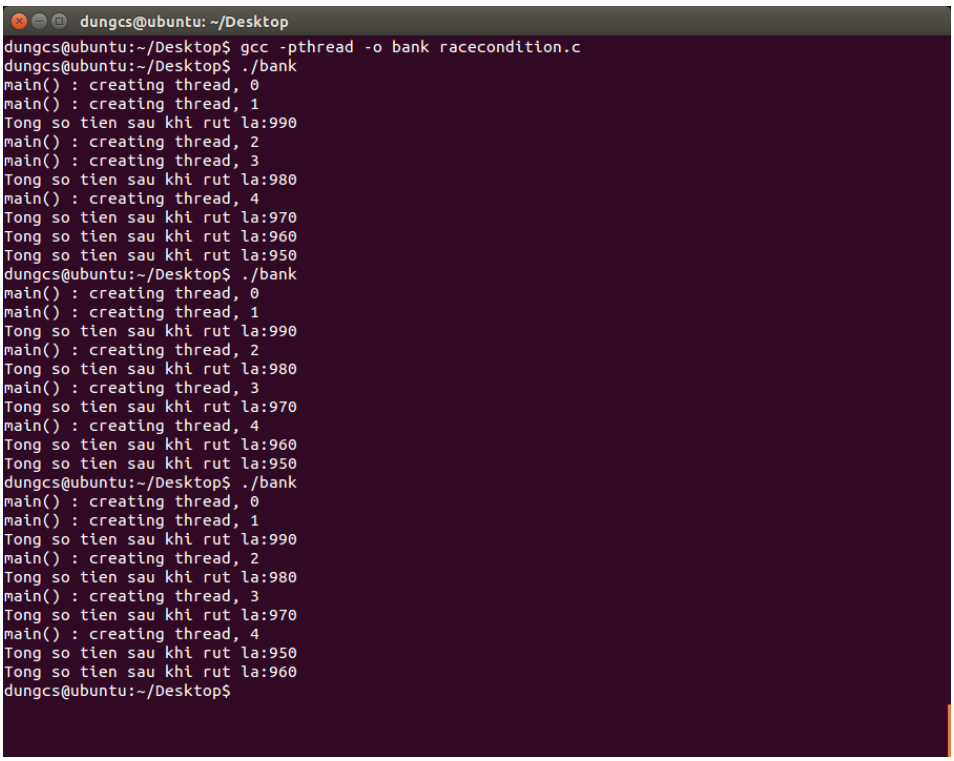
- Tài nguyên dùng chung có thể là một biến trên bộ nhớ, file,… (hay gặp nhất khi thao tác với file).

- Ví dụ: Người A có 1000 $ trong tài khoản, anh ta thực hiện rút 5 lần cùng lúc từ hệ thống banking mỗi lần 10$, như vậy trong tài khoản còn 950$. Đoạn code sau demo của ngân hàng thực hiện việc trừ tiền:



Tuy nhiên, thực tế không ra kết quả như vậy, trong 3 lần chạy thì có 1 lần sau khi rút 5 lần số tiền còn lại là 960$.

Nguyên nhân xảy ra hiện tượng này là vì thread thực hiện rút tiền lần 4 chưa kịp cập nhật tổng số tiền sau rút là 960 thì phải tạm dừng, 1 thread khác thực thi rút tiền lần thứ 5, số tiền còn lại là 950 được cập nhật. Sau đó thread rút tiền lần 4 cập nhật số tiền còn lại là 960. Như vậy sau 5 lần rút tiền, số tiền còn lại là 960$ - một kết quả sai.



3.1.2. Nguy cơ

- Thông thường lỗi sẽ dẫn đến chương trình chạy ra kết quả không đúng và có thể khác nhau với từng lần chạy

- Hacker có thể lợi dụng lỗi này để để thay đổi kết quả xử lý của chương trình theo hướng mang lại kết quả có lợi cho hacker (ví dụ ở trên).

- Chú ý: việc sử dụng đồng bộ có thể dẫn đến tình trạng deadlock - là hiện tượng 1 thread bị dừng/chờ, hoặc chạy lặp đi lặp lại 1 đoạn code mà nằm ngoài kiểm soát và kịch bản của chương trình.

3.1.3. Giải pháp

- Khi tác động các dữ liệu quan trọng, tiến hành khóa trước khi thực thi, đảm bảo dữ liệu tính toán và dữ liệu cập nhật là chính xác.

- Để chống trạng thái deadlock cần đảm bảo lệnh chờ/wait, vòng lặp phải tồn tại điều kiện thoát trong mọi trường hợp. Tránh trạng thái chờ đợi vòng tròn.

```c
int tientk;
pthread_mutex_t lock;
#define NUM_THREADS     100
int gettongtien() {
        return tientk;
}
void settongtien(int tongtien) {
        tientk=tongtien;
}
void *trutien(void* psotien) {
        int sotien=(int)psotien;
        pthread_mutex_lock(&lock);
        int tongtien=gettongtien();
        if (sotien <= tongtien) {
                tongtien=tongtien-sotien;
                settongtien(tongtien);
                printf("Tong so tien sau khi rut la:%d\n",gettongtien());

        } else {
                printf("Khong du tien de rut.");
        }
        pthread_mutex_unlock(&lock);
        pthread_exit(NULL);
}
int main() {
        tientk=1000;
        pthread_t threads[NUM_THREADS];
        int rc, i, sotien=10;
        if (pthread_mutex_init(&lock, NULL) != 0) {
                printf("\n mutex init failed\n");
                return 1;
        }
        for( i=0; i < NUM_THREADS; i++ ) {
                printf("main() : creating thread, %d\r\n", i) ;
                rc = pthread_create(&threads[i], NULL, trutien, (void *)sotien);
                if (rc) {
                        printf("Error:unable to create thread,%d\r\n",rc);return 0;
                }
        }
        pthread_exit(NULL);return 1;
}
```

- Khóa file của file khi thực thi nhằm tránh luồng hoặc tiến trình tác động vào file đang thao tác.

- VD: Code khóa file Linux

racecondition.c × | lockfile.c × | openreadonly.c × | testfile.txt

```c
#include <fcntl.h>
#include <stdio.h>
#include <string.h>
#include <unistd.h>
int main (int argc, char* argv[])
{
        char* file = argv[1];
        int fd;
        struct flock lock;
        printf ("opening %s\n", file);
        /* Open a file descriptor to the file. */
        fd = open (file, O_WRONLY);
        if (fd!=NULL)
                printf ("locking\n");
                /* Initialize the flock structure. */
                memset (&lock, 0, sizeof(lock));
                lock.l_type = F_WRLCK;
                /* Place a write lock on the file. */
                fcntl (fd, F_SETLKW, &lock);
                printf ("locked; hit Enter to unlock... ");
                /* Wait for the user to hit Enter. */
                getchar ();
                printf ("unlocking\n");
                /* Release the lock. */
                lock.l_type = F_UNLCK;
                fcntl (fd, F_SETLKW, &lock);
                close (fd);
        }
        return 0;
}
```

- VD: Code khóa file Windows

```
#include "stdafx.h"
#include <windows.h>
#include <stdio.h>
#include <stdlib.h>

int _tmain(int argc, _TCHAR* argv[])
{
    HANDLE hFile = ::CreateFileA("lockBlock.cpp", GENERIC_READ, FILE_SHARE_READ, 0, OPEN_EXISTING, 0, 0);
    OVERLAPPED overlapped;
    memset(&overlapped, 0, sizeof(overlapped));
    const int lockSize = 10000;
    printf("Taking lock\n");
    if (!LockFileEx(hFile, LOCKFILE_EXCLUSIVE_LOCK, 0, lockSize, 0, &overlapped))
    {
        DWORD err = GetLastError();
        printf("Error %i\n", err);
    }
    else
    {
        printf("Acquired lock\n");
        getchar();
        UnlockFileEx(hFile, 0, lockSize, 0, &overlapped);
        printf("Released lock\n");
    }
    return 0;
}
```

3.2. Tránh lỗi khi truy nhập file (TC.LTAT.CCPP.3.2; Bắt buộc)

3.2.1. Nguy cơ

- Khi tên file không lọc kí tự đặc biệt dạng ”/../” thì sẽ xảy ra lỗi path traversal cho phép hacker điều khiển chương trình đọc đến file khác với thiết kế của ứng dụng.

- Cần kiểm tra cả nội dung của file, đảm bảo đúng kích thước, định dạng và tính toàn vẹn trước khi sử dụng.

3.2.2. Giải pháp

- Với các tên file do người dùng nhập vào thì cần lọc các ký tự đặc biệt và kiểm tra thư mục tuyệt đối để tránh lỗi path traversal.

- Kiểm tra kích thước và tính toàn vẹn của dữ liệu trên file dữ liệu đọc từ đĩa.

- Kiểm tra extension và định dạng của file đảm bảo đúng định dạng cần đọc.

- Ví dụ kiểm tra đường dẫn và extension của file trên linux:

```
#include <iostream>
#include <string>
#include <limits.h>
#include <stdlib.h>

std::string getFileExt(std::string file_name)
{
   size_t index = file_name.rfind('.', file_name.length());
   if (index != std::string::npos)
   {
```

```
        return (file_name.substr(index + 1, file_name.length() - index));
    }

    return "";
}

bool checkPathTraversal(std::string file_name)
{
    const std::string config_dir = "/etc/myapp/";
    char realpath_result[PATH_MAX];

    // Get realpath
    char *result = realpath(file_name.c_str(), realpath_result);
    if (result == NULL) {
        std::cerr << "Realpath error " << errno << std::endl;
        return false;
    }

    // Check config dir
    if (std::string(realpath_result).find(config_dir) != 0)
    {
        std::cerr << "Invalid directory" << std::endl;
        return false;
    }

    return true;
}

int main()
{
    char file_name_buffer[PATH_MAX] = {0};

    // Read file name from stdin
```

```
    printf("Please input file name: ");
    char *result = fgets(file_name_buffer, sizeof(file_name_buffer), stdin);
    if (result == NULL) {
        std::cerr << "Cannot get file name" << std::endl;
        exit(1);
    }

    // Trim file name
    std::string file_name = file_name_buffer;
    if (file_name.length() && file_name.back() == '\n')
    {
        file_name = file_name.substr(0, file_name.length() - 1);
    }

    // Check file extension
    std::string extension = getFileExt(file_name);
    if (extension.compare("conf") != 0)
    {
        std::cerr << "Invalid file extension" << std::endl;
        exit(1);
    }

    // Check path traversal
    if (!checkPathTraversal(file_name))
    {
        std::cerr << "Check path traversal false" << std::endl;
        exit(1);
    }

    exit(0);
}
```

3.3. Sử dụng đường dẫn tuyệt đối khi nạp thư viện động (TC.LTAT.CCPP.3.3; Khuyến cáo)

3.3.1. Nguy cơ

- Khi chương trình nạp các thư viện động trong quá trình chạy, nếu đường dẫn của thư viện động được sử dụng không phải là đường dẫn tuyệt đối, thì thư viện mà chương trình nạp lên phụ thuộc vào biến môi trường, registry, thư mục hiện tại,... làm cho chương trình có thể nạp các thư viện không mong muốn do kẻ xấu điều khiển.

3.3.2. Giải pháp

- Khi nạp thư viện động nên truyền vào đường dẫn tuyệt đối của thư viện.

- Sử dụng hàm realpath() trên Unix/Linux và GetFullPathName() trên Windows.

- Ví dụ: Sử dụng hàm realpath()

```
char full_path[1024];
char *result = realpath(”my_lib.so”, full_path);
printf(”%s”, result);
```

3.4. Truy nhập đúng quyền (TC.LTAT.CCPP.3.4; Bắt buộc)

3.4.1. Nguy cơ

- Khi chương trình truy nhập các đối tượng (file, thư mục, Registry, event, mutex,…) với quyền lớn hơn nhu cầu cần thiết thì có nguy cơ khi chương trình bị lỗ hổng khác, hacker có thể điều hướng để tác động vào các đối tượng dễ dàng hơn.

- Ví dụ: Khi mở file cấu hình quan trọng chỉ để đọc thì chỉ cần mở file với quyền Read-Only, không cần sử dụng thêm quyền Write, tuy nhiên thường các lập trình viên mở luôn cả quyền Write. Điều này gây nguy cơ chương trình có thể có lỗi khác giúp hacker ghi đè vào file đó gây lỗi, hoặc nguy cơ cho chương trình.

3.4.2. Giải pháp

- Truy nhập đúng quyền cần thiết. Tuyệt đối tránh mở full quyền nếu không thực sự cần thiết.

- Ví dụ: Code mở file với quyền đọc trên Windows:

```
// Mở file chỉ để đọc, chỉ cần sử dụng quyền GENERIC_READ
HANDLE hFile = CreateFile(fileName, GENERIC_READ,
FILE_SHARE_READ, ...);
if (hFile == INVALID_HANDLE_VALUE)
{
        // Không mở được file
        ...
}
```

- Ví dụ: Code mở file với quyền đọc trên Linux

```
#include <iostream>
#include <unistd.h>
#include <fcntl.h>
#include <sstream>

using namespace std;

int main(int argc, char *argv[])
{
        char* file = argv[1];
        int fd;
        printf ("creating %s\n", file);
        /* open a file for readonly */
        fd = open (file, O_RONLY);
        if (fd!=NULL)
        {
                /*.... */
                close (fd);
        }
        return 0;
}
```

- Hạn chế quyền truy nhập: Khi tạo ra các đối tượng (file, thư mục, event, mutex,…) mà không muốn các ứng dụng, hệ thống khác có thể thao tác được với đối tượng, cần giới hạn quyền truy cập.

- Ví dụ: Code tạo file thư mục có chỉ định DACL giới hạn quyền truy cập trên Windows

```
// Ví dụ về tạo thư mục có chỉ định DACL


BOOL CreateMyDACL(SECURITY_ATTRIBUTES * pSA)
{
        TCHAR * szDACL = _T("D:")          // Tạo DACL
                _T("(D;OICI;GA;;;BG)")// Từ chối quyền truy cập với
                                        // tài khoản built-in guests
                _T("(D;OICI;GA;;;AN)") // Từ chối quyền truy cập với tài khoản
                                        // đăng nhập anonymous
                _T("(A;OICI;GRGWGX;;;AU)")       // Cho phép
read/write/execute với
                                        // các tài khoản đã đăng nhập
                _T("(A;OICI;GA;;;BA");         // Toàn quyền với tài khoản
administrators


        if (pSA == NULL)
                return FALSE;
```

```
        return ConvertStringSecurityDescriptorToSecurityDescriptor(
                        szDACL,
                        SDDL_REVISION_1,
                        &(pSA->lpSecurityDescriptor),
                        NULL);
}

SECURITY_ATTRIBUTES sa;

// Sử dụng SECURITY_ATTRIBUTES để gán DACL cho đối tượng
sa.nLength = sizeof(SECURITY_ATTRIBUTES);
sa.bInheritHandle = FALSE;

// Khởi tạo DACL cho đối tượng
if (CreateMyDACL(&sa))
{
        // Sử dụng DACL vừa tạo để kiểm soát quyền với thư mục cần tạo
        if (CreateDirectory(dirName, &sa))
        {
                ...
        }
}
```

- Ví dụ: Code tạo file chỉ đọc, giới hạn chỉ có user sở hữu file có quyền truy cập đọc ghi trên linux

```cpp
#include <iostream>
#include <unistd.h>
#include <fcntl.h>
#include <sstream>

using namespace std;

int main(int argc, char *argv[])
{
        char* file = argv[1];
        int fd;
        printf ("creating %s\n", file);
        /* create a file for read only, user (file owner)
        has read, write permission, if not exist. */
        fd = open (file, O_RONLY|O_CREAT,S_IRUSR|SIWUSR);
        if (fd!=NULL)
        {
                /*.... */
                close (fd);
        }
        return 0;
}
```

3.5. Tránh lỗi leak tài nguyên hệ thống (TC.LTAT.CCPP.3.5; Bắt buộc)

3.5.1. Nguy cơ

Khi một chương trình sử dụng các tài nguyên của hệ thống (file, memory, event, mutex,…) mà không giải phóng các tài nguyên sau khi sử dụng có thể dẫn đến:

- Gây tốn tài nguyên hệ thống có thể làm cạn kiệt tài nguyên dẫn đến không thể cấp phát mới.

- Khi chương trình bị tấn công và khai thác, các tài nguyên chưa giải phóng làm hacker có nhiều thông tin về hoạt động của hệ thống hơn, có thể khai thác hệ thống sâu hơn.

3.5.2. Giải pháp

- Thực hiện giải phóng tài nguyên ngay sau khi không cần sử dụng nữa, giải phóng càng sớm càng tốt. Ví dụ: sau khi mở file với hàm fopen_s thì phải sử dụng hàm fclose để giải phóng đối tượng trả về. Sau khi cấp phát bộ nhớ bằng hàm malloc thì phải giải phóng bằng hàm free.

- Chú ý: trường hợp hàm return nhiều chỗ, phải thực hiện close, giải phóng đầy đủ tất cả tài nguyên đã cấp phát trong các nhánh return.

```cpp
#include <stdio.h>


int main ()
{
    FILE * pFile;
    long file_size;
    char *buffer;
```

```
// Open file
errno_t err = fopen_s(&pFile, "myfile.txt","rb");
if (err != 0)
{
return 1;
}
// Get file length
fseek(pFile, 0, SEEK_END);
file_size = ftell(pFile);
if (!file_size) {
fclose(pFile);
return 1;
}

// Alloc memory
buffer = (char *) malloc (file_size + 1);
if (!buffer)
{
fclose(pFile);
return 1;
}

// Add null terminate
buffer[file_size] = 0;

fseek(pFile, 0, SEEK_SET);
fread(buffer, file_size, 1, pFile);

// Close file
fclose(pFile);
// Do something with buffer
```

```
        free(buffer);
        return 0;
}
```

4. Bảo mật khi giao tiếp, xác thực, phân quyền ứng dụng

4.1. Giao thức an toàn (TC.LTAT.CCPP.4.1; Bắt buộc)

4.1.1. Nguy cơ

- Trong các hệ thống thiết kế có các module giao tiếp với nhau thông qua mạng theo mô hình client-server, nhiều hệ thống cho phép cứ có kết nối đến cổng mở sẵn theo giao thức đã định nghĩa là làm việc mà không cần biết hệ thống nào đang giao tiếp với mình. Hacker có thể tiến hành dự đoán hoặc nghiên cứu giao thức thông qua dịch ngược ứng dụng phía client, dò quét các cổng mở, kết nối đến hệ thống và sau đó tác động trái phép đến hệ thống.

- Ví dụ:

Hệ thống đo đếm điện từ xa thiết kế theo mô hình client-server. Các sensor đọc chỉ số công tơ truyền qua mạng internet về một server tập trung tổng hợp, báo cáo xuất hóa đơn cho khách hàng. Để thực hiện được việc này, server phải lắng nghe trên 1 cổng, nhận dữ liệu từ client là sensor truyền về theo một giao thức đã định nghĩa sẵn. Nếu giao thức không có quá trình xác thực kết nối giữa client và server thì hacker có thể dò quét ra cổng trên server, từ đó gửi dữ liệu, thông tin hoặc tác động giả mạo lên server.

Trong nhiều hệ thống giao tiếp theo thông qua giao thức tầng ứng dụng dạng không giữ kết nối, các lệnh giao thức gửi từ client đến server luôn gửi kèm tài khoản và mật khẩu lên server trong mỗi lệnh. Điều này dẫn đến nguy cơ bị lộ mật khẩu khi hacker đứng giữa trên đường truyền hoặc thay đổi thông tin truyền nhận giữa client và server.

- Ví dụ:

Hệ thống đo đếm điện từ xa ở trên, thiết kế sử dụng giao thức dạng webservice không có mã hóa, mỗi request từ sensor gửi lên đều gửi kèm trường username + password. Hacker chặn bắt trên đường truyền có thể lấy luôn được username, password hoặc hacker đứng giữa thay đổi thông tin số liệu từ sensor gửi lên server. Từ đó hacker sử dụng công cụ gửi các request lên server sử dụng username, password đó giả mạo thiết bị sensor tác động vào hệ thống.

4.1.2. Giải pháp

- Giao thức ứng dụng dùng để giao tiếp giữa các module cần phải đảm bảo tính an toàn như:

  - Giao thức phải có xác thực kết nối giữa client với server.

- Giao thức cần phải có yếu tố duy trì phiên đã xác thực giữa client và server như sử dụng session duy trì phiên đăng nhập. Cách sinh và duy trì session như sau:
  - Client xác thực kết nối lần đầu với server. Server sinh ra bộ giá trị: sessionid thời gian hết hạn (timeout) lưu trữ trên server và gửi cho client, session (value) lưu trữ thông tin trên server về client kết nối lên server.
  - Client gửi các lệnh theo giao thức đã định nghĩa sẵn, trong đó có gửi cả trường sessionid lên server. Phía server kiểm tra nếu sessionid đúng, còn hiệu lực thì sẽ thực thi tiếp các lệnh theo giao thức.
  - Trường hợp session hết hạn, hoặc bị server từ chối, client cần phải thực hiện xác thực lại bằng username, mật khẩu.
- Với giao thức truyền qua mạng internet công cộng, có truyền thông tin quan trọng thì cần có mã hóa đường truyền. Thông thường sử dụng SSL/TLS.

- Ví dụ: Hệ thống đo đếm điện từ xa ở trên có thể thiết kế như sau đảm bảo giao thức an toàn:

- Sensor kết nối đến server thiết lập kết nối mã hóa sử dụng SSL/TLS.
- Sensor gửi request đăng nhập chứa username, password đến server.
- Server xác nhận đúng thông tin tài khoản. Tạo ra 1 session lưu trữ thông tin về phiên kết nối của client với thời gian timeout = thời gian hiện tại + 24h. Gửi cho client sessionid + timeout.
- Client gửi các lệnh, thông tin cần thiết thực hiện các chức năng, có kèm theo sessionid.
- Server kiểm tra thông tin session id, thời gian timeout. Nếu sai thì gửi lại thông báo lỗi về client. Nếu đúng thì thiết lập lại thời gian timeout của session, thực hiện các lệnh client gửi lên, gửi lại kết quả + thời gian timeout mới của session về client.

4.2. Xác thực an toàn (TC.LTAT.CCPP.4.2; Bắt buộc)

4.2.1. Nguy cơ

- Trong các hệ thống có yêu cầu xác thực người dùng trên máy của người dùng, nhiều hệ thống lưu trữ mật khẩu ở dạng rõ, hoặc dạng mã hóa 2 chiều. Hacker có thể dịch ngược chương trình, hoặc đôi khi chỉ cần tìm đúng file lưu trữ mật khẩu là có thể lấy được mật khẩu dạng rõ của người dùng.

- Với những hệ thống xác thực phía server thì hệ thống có thể gặp phải các nguy cơ về giao thức không an toàn như trong mục 4.1.

- Các thuật toán mã hóa 1 chiều yếu như MD5, SHA1 hiện nay dễ dàng bị bẻ khóa để tìm ra mật khẩu ở dạng rõ của người dùng.

4.2.2. Giải pháp

- Xây dựng cơ chế xác thực an toàn đảm bảo các yếu tố như:
    - Mã hóa 1 chiều mật khẩu kết hợp với yếu tố ngẫu nhiên salt khi cần lưu trữ mật khẩu.
    - Sử dụng giao thức an toàn khi xác thực trên server qua mạng. Tham khảo mục 4.1 “Giao thức an toàn“.
    - Sử dụng các thuật toán mã hóa 1 chiều mạnh từ SHA256 trở lên để mã hóa mật khẩu.

- Không ghi log các thông tin quan trọng của việc xác thực như mật khẩu, session id.

4.3. Phân quyền người dùng an toàn (TC.LTAT.CCPP.4.3; Bắt buộc)

4.3.1. Nguy cơ

- Trong các hệ thống có nhiều người dùng, nhiều hệ thống thực hiện phân quyền chức năng người dùng bằng cách thực hiện ẩn hiện các chức năng tùy theo loại người dùng. Ví dụ: Với người dùng đăng nhập là admin thì sẽ hiển thị các chức năng của admin. Với cách làm này, hacker có thể trực tiếp gọi, hoặc chỉnh sửa chương trình để gọi các chức năng chỉ có ở người dùng có quyền cao.

- Trong nhiều hệ thống, chương trình không kiểm tra xem người dùng đó có được phép xem hoặc tác động vào dữ liệu mà mặc định cứ dữ liệu nào hiển thị ra cho người dùng thao tác là dữ liệu được phép. Hacker có thể tác động làm chức năng thực thi trên dữ liệu của người dùng khác hoặc các dữ liệu không được phép.

4.3.2. Giải pháp

- Trong giai đoạn khảo sát, phân tích hệ thống cần phải xác định rõ yêu cầu của bài toán về quyền tác động vào các chức năng, các miền dữ liệu của từng loại người dùng. Từ đó, thiết kế các chức năng, phân hoạch dữ liệu cho phù hợp với yêu cầu phân quyền đó.

- Xây cơ chế đảm bảo mỗi người dùng chỉ được phép truy cập các chức năng, các dữ liệu mà mình được phép. Cơ chế phân quyền cần kiểm tra 2 câu hỏi trước khi thực hiện một chức năng hoặc một hành động: *Người dùng có được phép thực hiện chức năng đó hay không? Người dùng có được thao tác với dữ liệu đó hay không?*

4.4. Phân quyền module an toàn (TC.LTAT.CCPP.4.4; Khuyến cáo)

4.4.1. Nguy cơ

- Trong một hệ thống được phân chia thành nhiều module, có các module giao tiếp với người dùng hoặc với hệ thống khác, có các module xử lý dữ liệu,....

- Thông thường các module giao diện, giao tiếp với người dùng thường dễ dàng bị tấn công hơn các thành phần khác của hệ thống. Nếu các module này chạy với quyền cao (chẳng hạn như root) của hệ thống khi bị khai thác sẽ giúp hacker có nhiều quyền để tác động sâu vào hệ thống làm hậu quả nghiêm trọng hơn.

4.4.2. Giải pháp

- Chỉ dùng quyền tối thiểu cần thiết để chạy các thành phần của hệ thống.

- Không nên dùng quyền cao (admin/root) để chạy các module có giao diện, giao tiếp với người dùng hoặc với hệ thống khác và các module có nguy cơ bị tấn công cao.

5. Khuyến cáo khác

5.1. Sử dụng an toàn biến môi trường (TC.LTAT.CCPP.5.1; Khuyến cáo)

5.1.1. Nguy cơ

- Sử dụng một số hàm mặc định của C/C++ như getenv, putenv, setenv,... sẽ truy cập, tác động đến 1 vùng nhớ chứa các biến môi trường được chia sẻ. Vùng nhớ này có thể bị hacker lợi dụng lỗ hổng để thay đổi. Dẫn đến kết quả thực thi của chương trình có thể bị ảnh hưởng, gây hại cho chương trình.

5.1.2. Giải pháp

- Hạn chế cho người dùng tác động vào biến môi trường chạy của chương trình.

- **Với Windows**: Khuyến cáo nên sử dụng các Windows API để xử lý biến môi trường: GetEnvironmentVariable(), GetEnvironmentStrings(), SetEnvironmentVariable().

  - Nên sử dụng hàm GetEnvironmentVariable() để lấy biến môi trường:

```
TCHAR pathEnv[MAX_PATH + 10];
DWORD returnValue;

returnValue = GetEnvironmentVariable(_T(“PATH”), pathEnv,
MAX_PATH)
```

  - Hàm GetEnvironmentStrings() trả về con trỏ trực tiếp tới biến môi trường của tiến trình. Vùng nhớ trỏ bởi con trỏ này chỉ được truy nhập với quyền đọc (Read-only). Sau khi sử dụng xong vùng nhớ phải giải phóng bằng hàm FreeEnvironmentStrings().

```
TCHAR* env = GetEnvironmentString();

// Chỉ được đọc, không được phép ghi vào vùng nhớ trỏ bởi biến env
…

// Giải phóng bộ nhớ
```

```
FreeEnvironmentStrings(env);
```

- Nên sử dụng hàm SetEnvironmentVariable() để thiết lập biến môi trường:

```
TCHAR pathEnv[MAX_PATH + 10];


…
if (SetEnvironmentVariable(_T(“PATH”), pathEnv))
{
        …
}
```

- **Với Linux:** Nên sử dụng một vùng nhớ đệm để lưu trữ, hoặc thao tác biến môi trường, tách biệt với vùng nhớ biến môi trường chung.

Ví dụ: Code Sau khi getenv, copy vào 1 buffer biến môi trường để sử dụng cho chương trình.

```c
#include <stdio.h>      /* printf */
#include <stdlib.h>     /* getenv */
#include <limits.h>
#include <string.h>
int main ()
{
        char* pPath;
        char bufEnv[PATH_MAX];
        pPath = getenv ("PATH");
        strncpy(bufEnv,pPath,PATH_MAX-1);
        if (pPath!=NULL) {
                printf ("The current path is: %s",bufEnv);
                /*....*/
        }
  return 0;
}
```

5.2. Kiểm tra giá trị hàm trả về (TC.LTAT.CCPP.5.2; Bắt buộc)

5.2.1. Nguy cơ:

- Khi thực hiện các hàm, có thể kết quả chạy không đúng theo như luồng chính của chương trình có thể dẫn đến nhiều ngoại lệ rẽ nhánh. Việc không kiểm tra giá trị trả về có thể dẫn đến các chương trình chạy sai, truy cập vùng nhớ null, sinh ngoại lệ,... có thể dẫn đến các lỗi về bộ nhớ như use after free.

5.2.2. Giải pháp:

- Khi sử dụng các hàm có trả về giá trị, cần kiểm tra giá trị trả về đảm bảo quá trình gọi hàm không bị lỗi.

- Ví dụ:

```
hFile = CreateFile(…);
```

```
// Kiểm tra giá trị trả về
if (hFile == INVALID_HANDLE_VALUE) return;
ReadFileContent();
```

5.3. Không kết nối trực tiếp từ ứng dụng client đến server database tập trung (TC.LTAT.CCPP.5.3; Bắt buộc)

5.3.1. Nguy cơ:

- Với các ứng dụng nhiều người dùng, sử dụng trực tiếp cổng, tài khoản kết nối đến server database tập trung gây nguy cơ có thể lộ tài khoản kết nối đến database (hacker có thể dịch ngược để lấy), khi đó hacker có thể kết nối thẳng vào cơ sở dữ liệu.

5.3.2. Giải pháp:

- Xây dựng server xử lý trung gian đảm bảo có xác thực, phân quyền theo từng tài khoản người dùng. Ví dụ: Dựng webservice.

5.4. Sử dụng các công cụ phân tích mã nguồn để phát hiện các lỗi lập trình (TC.LTAT.CCPP.5.4; Khuyến cáo)

5.4.1. Nguy cơ:

- Trình biên dịch không thể phát hiện ra hết tất cả các lỗi cũng như nguy cơ bảo mật trong chương trình.

5.4.2. Giải pháp:

- Sử dụng các công cụ phân tích mã nguồn có sẵn của IDE như Code Analysis của Visual Studio, Code Analysis (Codan) trên Eclipse CDT,....

- Sử dụng các công cụ phân tích mã nguồn khác như: Flawfinder, Cppcheck,....

5.5. Không sử dụng các hàm bị đánh dấu obsolete (TC.LTAT.CCPP.5.5; Bắt buộc)

5.5.1. Nguy cơ:

- Các hàm đánh dấu là obsolete có thể do một số nguyên nhân như:
  - Không còn được hỗ trợ bởi một hay nhiều dòng hệ điều hành.
  - Hoạt động khác nhau trên các hệ điều hành khác nhau.
  - Có lỗ hổng bảo mật.
- Vì vậy sử dụng các hàm này không đảm bảo tính an toàn, ổn định và khả chuyển cho chương trình.

5.5.2. Giải pháp:

- Sử dụng các hàm khác để thay thế cho các hàm bị đánh dấu obsolete.

- Danh sách các hàm thay thế tham khảo **Mục 6. Danh sách các hàm thay thế trong lập trình an toàn sử dụng ứng dụng C/C++.**

- Ví dụ: Sử dụng hàm nanosleep thay thế cho hàm usleep

Nên	Không nên

int main()
{
// Sleep 1 second
struct timespec time_interval;
time_interval.tv_sec = 1;
time_interval.tv_nsec = 0;
nanosleep(&time_interval, NULL);
return 0;
}
	int main()
	{
	// Sleep 1 second
	usleep(1 * 1000 * 1000);
	return 0;
	}

5.6. Sửa hết cảnh báo (warning) khi biên dịch chương trình (TC.LTAT.CCPP.5.6; Khuyến cáo)

5.6.1. Nguy cơ:

- Các cảnh báo khi biên dịch không phải là lỗi, chương trình biên dịch vẫn thành công nhưng ẩn chứa các nguy cơ như:
    - Sử dụng các hàm không an toàn, như các hàm strcpy, gets,....
    - So sánh các kiểu dữ liệu không cùng kích thước, tính chất như so sánh số nguyên không dấu và có dấu.
    - Ép kiểu dữ liệu không an toàn.
    - Khai báo biến mà không sử dụng hoặc sử dụng biến chưa khởi tạo giá trị.
- Các cảnh báo này có thể cảnh báo trước rằng chương trình có thể hoạt động không đúng hoặc bị khai thác lỗ hổng.

5.6.2. Giải pháp:

- Sửa hết các cảnh báo khi biên dịch chương trình.
- Nên khởi tạo giá trị các biến trước khi sử dụng.
- Với các cảnh báo sử dụng hàm không an toàn, sử dụng các hàm thay thế trong **PHỤ LỤC 04**.

5.7. Tránh khai báo các mảng tĩnh có kích thước lớn trong hàm (TC.LTAT.CCPP.5.7; Khuyến cáo)

5.7.1. Nguy cơ

- Mỗi luồng trong tiến trình đều có stack với kích thước hữu hạn, đặc biệt là các driver hoạt động ở mức kernel chỉ có kích thước tối đa đến vài chục KB. Vì vậy việc sử dụng hợp lý tài nguyên stack là một yếu tố quan trọng để chương trình hoạt động ổn định và tránh bị đổ vỡ.

- Khi khai báo biến hoặc mảng trong một hàm, chúng sẽ được đặt trong stack khi tiến trình được chạy. Nếu khai báo một mảng tĩnh có kích thước quá lớn, chúng có thể gây tràn stack dẫn đến đổ vỡ chương trình hay hệ thống.

5.7.2. Giải pháp

- Không sử dụng mảng tĩnh có kích thước lớn, thay thế bằng các mảng được cấp phát động hoặc dùng std::vector.

Nên	Không nên

void func()
{
int* foo = new int[1000];
…
delete[] foo;
}
 	
Hoặc
 	
void func()
{
std::vector<int> foo(1000);
…
}
	void func()
	{
	int foo[1000];
	
	…
	}

5.8. Đảm bảo máy tính lập trình tuân thủ các Tiêu chuẩn ATTT cho máy tính người dùng cuối (TC.LTAT.CCPP.5.8; Bắt buộc)

5.8.1. Nguy cơ

- Nếu không thiết lập đầy đủ các Tiêu chuẩn ATTT, máy tính người dùng có cơ mất ATTT, dễ dàng bị tấn công và lộ lọt thông tin.

- Máy tính dùng để lập trình nếu bị tấn công có thể dẫn đến lộ lọt các thông tin quan trọng: mã nguồn, thiết kế hệ thống,.... Ngoài ra hacker có thể thay đổi mã nguồn hoặc file thực thi để phát tán mã độc.

5.8.2. Giải pháp

- Các máy tính lập trình và toàn bộ máy tính người dùng phải tuân thủ thiết lập đầy đủ các Tiêu chuẩn ATTT cho máy tính người dùng cuối mà Tập đoàn đã ban hành.

6. Danh sách các hàm thay thế trong lập trình an toàn sử dụng ứng dụng C/C++

Các hàm không an toàn	Hàm an toàn thay thế
Các hàm vào ra stream	
sscanf	sscanf_s
swscanf	swscanf_s
scanf	scanf_s
wscanf	wscanf_s
printf	printf_s
wprintf	wprintf_s
fscanf	fscanf_s
fwscanf	fwscanf_s
fopen	fopen_s
_wfopen	_wfopen _s
_sopen	_sopen_s
_wsopen	_wsopen _s
freopen	freopen_s
_wfreopen	_wfreopen _s
fprintf	fprintf _s
fwprintf	fwprintf _s
fscanf	fscanf_s
fwscanf	fwscanf _s
gets	gets_s
getws	getws _s
_access	_access_s
_waccess	_waccess_s

Các hàm không an toàn	Hàm an toàn thay thế
_makepath	_makepath_s
wmakepath	wmakepath _s
_mktemp	_mktemp_s
_wmktemp	_wmktemp_s
_splitpath	_splitpath_s
_wsplitpath	_wsplitpath_s
_umask	_umask _s

Các hàm làm việc với string	
sprintf	sprintf_s
swprintf	swprintf_s
vsprintf	vsprintf_s
vswprintf	vswprintf_s
strcat	strcat_s
wcscat	wcscat_s
strlen	strlen_s
strnlen	strnlen_s
wcslen	wcsnlen_s
_strlwr	_strlwr_s
_wcslwr	_wcslwr_s
strncat	strncat_s
wcsncat	wcsncat_s
strcpy	strcpy _s
wcscpy	wcscpy _s

strncpy	strncpy _s
wcsncpy	wcsncpy_s
strtok	strtok _s
wcstok	wcstok _s
_strupr	_strupr _s
_wcsupr	_wcsupr_s
vsnprintf	vsnprintf _s
_vsnwprintf	_vsnwprintf_s
RtlStringCchCopyA	RtlStringCbCopyA
RtlStringCchCatA	RtlStringCbCatA
RtlStringCchLengthA	RtlStringCbLengthA
RtlStringCchPrintfA	RtlStringCbPrintfA
RtlStringCchVPrintfA	RtlStringCbVPrintfA
RtlStringCchCopyW	RtlStringCbCopyW
RtlStringCchCatW	RtlStringCbCatW
RtlStringCchLengthW	RtlStringCbLengthW
RtlStringCchPrintfW	RtlStringCbPrintfW
RtlStringCchVPrintfW	RtlStringCbVPrintfW

Các hàm làm việc với bộ đệm	
memcpy	memcpy_s
wmemcpy	wmemcpy_s
memmove	memmove_s
wmemmove	wmemmove _s
Các hàm chuyển đổi dữ liệu	

_ecvt	_ecvt_s
_gcvt	_gcvt_s
_itoa	_itoa_s
_ui64toa	_ui64toa_s
itow	_itow_s
_i64tow	_i64tow_s
_ui64tow	_ui64tow_s
_ltoa	_ltoa_s
_ltow	_ltow_s
mbstowcs	mbstowcs_s
_mbstowcs_l	_mbstowcs_s_l
_ultoa	_ultoa_s
_ultow	_ultow_s
wctomb	wctomb_s
_wctomb_l	_wctomb_s_l
Các hàm được đánh dấu obsolete	
getpass	Tự cài đặt
gsignal, ssignal	raise/signal
memalign	malloc
ulimit	getrlimit, setrlimit, sysconf
usleep	nanosleep, setitimer
Các hàm tạo tiến trình	
execl, execlp, execle, execv, execvp, system, popen	execve với POSIX CreateProcess với Windows
WinExec, ShellExecute	CreateProcess

Phụ lục 04.
HƯỚNG DẪN LẬP TRÌNH AN TOÀN CHO ỨNG DỤNG ỨNG DỤNG IOS VÀ ANDROID

- Định nghĩa:

+ Sql lite: Hệ quản trị cơ sở dữ liệu SQL Lite.

+ Máy điện thoại bị root: Các ứng dụng sẽ chạy với đặc quyền cao nhất.

+ MODE_WORLD_ READABLE: Ở chế độ này tất cả các ứng dụng chỉ có quyền đọc.

+ MODE_PRIVATE: Các file được tạo ra do ứng dụng thì chỉ có ứng dụng đó mới được đọc file này.

+ MODE_WORLD_ WRITEABLE: Ở chế độ này tất cả các ứng dụng chỉ có quyền ghi.

+ Share Preference: Nó là một chức năng của hệ điều hành Android.

+ Activity: thành phần xử lý giao diện của ứng dụng Android.

+ Service: Thành phần xử lý các tác vụ chạy nền của ứng dụng Android.

+ Broadcast Receiver: thành phần nhận sự kiện, thông báo của ứng dụng Android.

+ Content Provider: thành phần xử lý việc lưu trữ dữ liệu của ứng dụng android.

- Thuật ngữ:

+ XSS (Cross Site Scripting): Kiểu tấn công nhắm vào phía người dùng như đánh cắp thông tin truy cập, hướng người dùng vào các trang web có mã độc...

+ TapJacking: Xảy ra khi một ứng dụng độc hại cài đặt trên điện thoại chạy Android tạo ra các giao diện giả mạo người dùng nhằm lừa người dùng mua hàng, nhấp vào quảng cáo, cài đặt các ứng dụng, hoặc thậm chí xóa sạch tất cả các dữ liệu từ điện thoại...

+ Client injection: Những phương pháp tấn công chèn mã độc vào từ phía người dùng.

+ SQL Injection: Phương pháp tấn công chèn dữ liệu vào các câu truy vấn sql.

+ Hardcode: Các dữ liệu được đặt vào trong mã nguồn và không thay đổi.

+ Session, Cookie: Phiên đăng nhập của người dùng.

1. Bảo vệ các dữ liệu được lưu trữ trên di động

1.1 Không sử dụng tính năng ghi nhớ mật khẩu cho các ứng dụng quan trọng.

- **Nguy cơ:** Khi sử dụng chức năng ghi nhớ mật khẩu có thể bị lộ thông tin trong trường hợp mất điện thoại.

1.2 Phân quyền, mã hóa dữ liệu lưu trữ trên thiết bị.

- **Nguy cơ:** Các dữ liệu lưu trữ tạm thời trong điện thoại ở dạng file hay sql lite đều có thể bị lộ nếu mất điện thoại, máy đã bị root ...

- **Khuyến cáo:** Hạn chế lưu trữ thông tin trên điện thoại, chỉ lưu những thông tin quảng bá. Không lưu trữ các dữ liệu quan trọng như: tài khoản, mật khẩu, mã PIN ... dưới dạng rõ, có thể sử dụng thêm Keychain của iOS, và keystore của Android để tăng tính bảo mật. Mật khẩu có thể được mã hóa bằng các thuật toán AES (độ dài key >= 256 bit), RSA (độ dài key >= 2048 bit) hoặc các thuật toán tương đương trước khi lưu để đảm bảo an toàn.

- **Yêu cầu:** Các dữ liệu, tài liệu mật của Tập đoàn lưu trữ trên thiết bị di động cần được mã hóa bảo vệ.

+ Trên Android: Không sử dụng quyền world readable và writable khi lưu các thông tin quan trọng.

Ví dụ: Đoạn chương trình sau sử dụng Share Preference để lưu thông tin đăng nhập của người dùng.

```
public void saveCredentials(String userName, String password) {

    SharedPreferences credentials = this.getSharedPreferences(
            "credentials", MODE_WORLD_READABLE);
    SharedPreferences.Editor editor = credentials.edit();
    editor.putString("username", userName);
    editor.putString("password", password);
    editor.putBoolean("remember", true);
    editor.commit();
}
```

Nếu khai báo với thuộc tính "MODE_WORLD_READABLE" như trên thì bất cứ ứng dụng nào cũng có thể đọc được thông tin username và password này. Để không cho phép các ứng dụng khác đọc được thông tin này cần thay thuộc tính "MODE_WORLD_ READABLE" thành "MODE_PRIVATE".

+ Trên IOS: Cần phân loại dữ liệu ứng dụng theo các mức độ bảo mật khác nhau và lưu trữ chúng trong các thư mục có vai trò tương ứng trong ứng dụng. Bảng mô tả vai trò các thư mục thông thường trong ứng dụng:

Thư mục	Mô tả
Application.app	*Lưu trữ các nội dung cố định của ứng dụng và mã thực thi của ứng dụng. Các nội dung này được ký và kiểm tra khi thực thi*
Documents	*Là nơi lưu trữ các dữ liệu thường xuyên cho ứng dụng; dữ liệu trong thư mục này được đồng bộ và sao lưu với iTunes.*

Thư mục	Mô tả
Library	*Thư mục này chứa các dữ liệu hỗ trợ cho ứng dụng thực thi như file cấu hình, tham chiếu, dữ liệu cache, cookies.*
tmp	*Lưu trữ các file tạm.*

Khi thao tác với các dữ liệu loại dữ liệu có mức bảo mật khác nhau cần sử dụng các class chuẩn và tùy chọn tương ứng của thư viện lập trình cho iOS. Bảng mô tả mức độ bảo mật dữ liệu, class chuẩn và tùy chọn bảo mật tương ứng trong thư viện lập trình iOS.

Mức bảo mật	Mô tả	NSData	NSFileManager
No Protection	File không mã hóa. Dùng lưu trữ những dữ liệu tạm, không quan trọng.	NSDataWritingFileProtectionNone	NSFileProtectionNone
Complete Protection	File được mã hóa và không thể truy cập khi thiết bị ở trạng thái lock. Dùng lưu trữ các dạng dữ liệu cần bảo vệ cao, khi lock máy thì không cho phép truy cập dữ liệu	NSDataWritingFileProtectionComplete	NSFileProtectionComplete
Complete Unless Open	File được mã hóa. Khi file đang được mở bởi một ứng dụng mà thiết bị chuyển sang trạng thái lock thì chỉ ứng dụng đó được tiếp tục thao tác với file cho đến khi đóng, còn các ứng dụng khác không thể truy cập đến file. Giống dạng Complete Protection, tuy nhiên cho phép các ứng dụng đang thao tác với file được thực thi tiếp , phù hợp với các trường hợp như đang download.	NSDataWritingFileProtectionCompleteUnlessOpen	NSFileProtectionCompleteUnlessOpen
Complete Until First User Authentication	File được mã hóa và không thể truy cập cho đến khi lần đầu unlock thiết bị sau khi khởi động máy. Dùng để bảo vệ dữ liệu khỏi các kiểu tấn	NSDataWritingFileProtectionCompleteUntilFirstUserAuthentication	NSFileProtectionCompleteUntilFirstUserAuthentication

Mức bảo mật	Mô tả	NSData	NSFileManager
	công cần khởi động lại máy.		

1.3 Bảo vệ dữ liệu nhạy cảm khi ứng dụng chạy chế độ nền

- Nguy cơ: Khi ứng dụng chuyển sang chế độ chạy nền, có thể có nhiều thông tin hiển thị trên giao diện có thể bị lộ nếu người dùng không tắt hoàn toàn ứng dụng và người nào đó có thể vô tình nhìn thấy. Ví dụ: Khi đang nhập thông tin thẻ tín dụng.

- Khuyến cáo: Với những trường hợp cần đảm bảo dữ liệu không bị lộ sau khi chuyển sang chạy nền thì cần bắt sự kiện ứng dụng chuyển sang chế độ chạy nền để ẩn các thông tin này đi.

Ví dụ: Trên IOS để ẩn thông tin một ô text sau khi ứng dụng chuyển sang chạy nền:

Objective-C:

```
- ( void)applicationDidEnterBackground:(UIApplication*) application
{       viewController.creditcardNumber.hidden = YES;
}
- (void)applicationDidBecomeActive:(UIApplication *) application {
        viewController.creditcardNumber.hidden = NO;
}
```

Swift:

```
func applicationDidEnterBackground(_ application: UIApplication) {
    viewController.creditcardNumber.isHidden = true
}

 func applicationDidBecomeActive(_ application: UIApplication) {
   viewController.creditcardNumber.isHidden = false
}
```

2. Bảo mật giao tiếp giữa ứng dụng và máy chủ

- Nguy cơ: Hầu hết các ứng dụng di động đều có kết nối tới máy chủ đặt trên Internet để cập nhật, trao đổi thông tin. Quá trình truyền nhận tin này có thể bị nghe lén từ mạng viễn thông, mạng Wifi…

- Yêu cầu: Các thông tin quan trọng khi truyền giữa ứng dụng và máy chủ (Như quá trình đăng nhập, cookie, session …) phải được mã hóa.

- Khuyến cáo: Nên sử dụng các giao thức chuẩn như HTTPS, SSL/TLS có SSL Pinning (kiểm tra chính xác chứng thư số hoặc public key trong các cert server trả về tương ứng với host kết nối) để đảm bảo an toàn và chống hacker tấn công nghe lén sử dụng các phương thức như fake dns hay import cert vào trusted CA trên thiết bị người dùng.

+ Trên IOS: có thể sử dụng SSL/TLS thông qua các class như NSURLConnection, NSURLRequest, NSURLResponse. Ví dụ: Tạo một kết nối HTTPS như sau:

Objective-C:

```
@implementation insecuressl
int main(int argc, const char* argv[])
{
        NSString *myURL=@"https://localhost/test";
        NSURLRequest *theRequest = [NSURLRequest
requestWithURL:[NSURL URLWithString:myURL]];
        NSURLResponse *resp = nil;
        NSError *err = nil;
        NSData *response = [NSURLConnection sendSynchronousRequest:
        theRequest returningResponse: &resp error: &err];
        NSString * theString = [[NSString alloc] initWithData:response
encoding:NSUTF8StringEncoding];
        [resp release];
        [err release];
        return 0;
}
```

Swift:

```
func callHttp()
{
      var request = URLRequest(url:URL(string:urlConnect)!)
      let config = URLSessionConfiguration.default
      let task = URLSession.shared.dataTask(with: request)
      {
         data, response, error in
         guard let data = data, error == nil else {
```

```
            return
        }

        let responseString = String(data: data, encoding: .utf8)
        // Do something
    }
    task.resume()
}
```

+ Trên Android Ví dụ: Tạo một kết nối HTTPS như sau.

```
URL url = new URL("https://bank.com/authen");
HttpsURLConnection urlConn =
(HttpsURLConnection)url.openConnection();
```

Hoặc

```
HttpsURLConnection urlConn = new
HttpsURLConnection("https://bannk.com/authen ");
```

3. Bảo mật xác thực người dùng

3. 1 Áp dụng chính sách mật khẩu mạnh

- Nguy cơ: Khi không có sự bắt buộc sử dụng mật khẩu mạnh, người dùng thường sử dụng các mật khẩu đơn giản, dễ nhớ. Điều này dẫn đến nguy cơ hacker có thể đoán được mật khẩu của người dùng một cách dễ dàng.

- Yêu cầu: Áp dụng chính sách mật khẩu mạnh đối với tất cả các hệ thống nội bộ.

- Khuyến cáo: Đối với các hệ thống phục vụ khách hàng bên ngoài, có thể không áp đặt chính sách mật khẩu mạnh bắt buộc nhưng nên cảnh báo người dùng nếu họ sử dụng mật khẩu yếu.

Ví dụ: Hàm bên dưới kiểm tra 1 mật khẩu có thỏa mãn điều kiện dài ít nhất 10 ký tự; bao gồm cả chữ, số, kí tự đặc biệt hay không:

```
public static boolean isStrongPassword(String password) {
String pattern = "((?=.*[0-9])(?=.*[a-zA-Z])(?=.*[@#$%^&+=]).{8,})";
    return password.matches(pattern);
}
```

3. 2 Bảo mật trong lưu trữ mật khẩu trên thiết bị.

- Nguy cơ: Nếu ứng dụng tự lưu trữ mật khẩu trên thiết bị bằng các đoạn mã tự viết thì có nguy cơ rất cao trong việc để lộ mật khẩu.

- Khuyến cáo: Nên sử dụng cơ chế sẵn có của iOS/Android cho phép để lưu trữ mật khẩu là keychain/Keystore. Mật khẩu có thể được mã hóa bằng các thuật toán AES (độ dài key >= 256 bit), RSA (độ dài key >= 2048 bit) hoặc các thuật toán tương đương trước khi lưu để đảm bảo an toàn. Nếu thiết bị hỗ trợ xác thực vân tay, nên sử dụng để thay thế cho việc nhập mật khẩu của người dùng, vừa giúp thuận tiện cho việc sử dụng của người dùng, vừa tránh việc để lộ mật khẩu khi người dùng gõ mật khẩu.

3. 3 Áp dụng xác thực đa yếu tố khi truy cập vào các hệ thống quan trọng.

- Nguy cơ: Chỉ bảo vệ truy nhập ứng dụng bằng mật khẩu thì hacker có thể dễ dàng đăng nhập vào tài khoản của người dùng khi người dùng để lộ mật khẩu, hoặc hacker sử dụng các phương pháp như phishing, bruteforce, keylogger... để ăn cắp mật khẩu người dùng.

- Khuyến cáo: Đối với các hệ thống quan trọng nên bổ sung thêm một lớp xác thực nhập mã OTP (qua SMS hoặc USSD, GoogleAuthen) để đảm bảo an toàn cho người dùng.

4. Bảo vệ tấn công phía client injection và tapjacking

4. 1 Kiểm soát truy vấn cơ sở dữ liệu để tránh lỗ hổng SQL Injection

- Nguy cơ: Khi truy vấn tới cơ sử dữ liệu lập trình viên thường sử dụng cách cộng xâu Input từ người dùng, các câu truy vấn này có thể bị mắc lỗi SQL. Bằng việc lợi dụng lỗi này, kẻ tấn công có thể xem, thêm, sửa, xóa dữ liệu, lấy cắp thông tin người dùng...

- Yêu cầu: Truy vấn SQL phải dùng PrepareStatement, tất cả tham số phải được thêm bằng hàm (setParam..), không được sử dụng cách cộng xâu trong truy vấn.

+ Trên Android: Ví dụ: Đoạn code kiểm tra đăng nhập với username/password do người dùng nhập vào

```
String username = Username.getText().toString();
String password = Password.getText().toString();
SQLiteDatabase db = mDbHelper.getWriteableDatabase();
String userQuery = "SELECT * FROM useraccounts WHERE user_name = '" + username + "' and password = '" + password + "'";
SQLiteStatement prepStatement = db.compileStatement(userQuery);
```

Nhập vào username là test' or '1'='1 thì câu query sẽ là: select * from useraccounts where user_name='test' or '1'='1' and password='...'. Mệnh đề where sẽ luôn đúng. Như vậy dù không có password vẫn đăng nhập được vào hệ thống.

Đoạn code bên dưới, username, password được tham số hóa khi đưa vào câu truy vấn nên tránh được lỗi SQL Injection.

```
SQLiteDatabase db = mDbHelper.getWriteableDatabase();
String userQuery = "SELECT * FROM useraccounts WHERE user_name = ? and password = ?";
prepStatement.bindString(1,Username.getText().toString()("user_name");
prepStatement.bindString(2,Username.getText().toString()("password"));
SQLiteStatement prepStatement = db.compileStatement(userQuery);
```

+ Trên IOS: Ví dụ: Tham số hóa tất cả các tham số khi query SQL.

Objective-C:

```
sqlite3 *database;
sqlite3_stmt *statement;
if(sqlite3_open([databasePath UTF8String], &database) != SQLITE_OK) {
    // error opening database
    return
}
if(sqlite3_prepare_v2(database, insert_stmt, -1, &statement, NULL) == SQLITE_OK) {
    const char *insert_stmt = "INSERT INTO messages VALUES('1', ?, ?, ?)";
    sqlite3_prepare_v2(database, insert_stmt, -1, &statement, NULL);
    sqlite3_bind_text(&insert_stmt, 1, [msg UTF8String], -1, SQLITE_TRANSIENT);
    sqlite3_bind_text(&insert_stmt, 2, [user UTF8String], -1, SQLITE_TRANSIENT);
    sqlite3_bind_text(&insert_stmt, 3, [displayname UTF8String], -1, SQLITE_TRANSIENT);
    if (sqlite3_step(statement) == SQLITE_DONE) {
       // do something
    }
}
sqlite3_finalize(&statement)
```

Swift:

```
var database: OpaquePointer?
```

```
if sqlite3_open(databasePath.path, &database) != SQLITE_OK {
    // error opening database
    return
}
var statement: OpaquePointer? = nil
let insert_stmt: String = "INSERT INTO messages VALUES('1', ?, ?, ?))"
if sqlite3_prepare_v2(database, insert_stmt, -1, &statement, nil) ==
SQLITE_OK {

    sqlite3_bind_text(insert_stmt, 1, msg, -1, nil)
    let msgUtf8 = String(utf8String: msg.cString(using: .utf8)!)
    let userUtf8 = String(utf8String: user.cString(using: .utf8)!)
    let displaynameUtf8 = String(utf8String: displayname.cString(using:
.utf8)!)
    sqlite3_bind_text(insert_stmt, 1, msgUtf8, -1, nil)
    sqlite3_bind_text(insert_stmt, 1, userUtf8, -1, nil)
    sqlite3_bind_text(insert_stmt, 1, displaynameUtf8, -1, nil)

    if sqlite3_step(statement) == SQLITE_DONE {
       // do something
    }
}
sqlite3_finalize(statement)
```

4. 2 Ngăn chặn lỗi XSS

- Trên Android:

+ Nguy cơ: Mặc định webview đã tắt không cho phép thực thi javascript, nhưng nếu lập trình viên thiết lập thuộc tính setJavaScriptEnabled(true) thì webview sẽ cho phép thực thi javascipt và có thể bị khai thác lỗi xss.

+ Khuyến cáo: Khi sử dụng webview không thiết lập thuộc tính setJavaScript Enabled(true) nếu không cần sử dụng đến javascript.

Ví dụ: Đoạn chương trình phía dưới sử dụng webview để hiển thị website có địa chỉ là http://www.malicious.com. Như vậy nếu kẻ tấn công lợi dụng khai thác lỗi xss trên site này và chèn mã javascript vào thì ứng dụng có thể bị khai thác thông qua lỗi xss của site này.

```
...
WebView myWebView = (WebView) findViewById(R.id.webview);
WebSettings webSettings = myWebView.getSettings();
webSettings.setJavaScriptEnabled(true);
myWebView.loadUrl("http://www.malicious.com");
...
```

- Trên IOS:

+ Nguy cơ: Khi sử dụng hàm ”stringByEvaluatingJavaScriptFromString” để truyền dữ liệu vào cho javascript hiển thị trên UIWebViews thì dữ liệu truyền vào có thể chứa script thực thi gây ra lỗi XSS cho phép thực thi rất nhiều hành động nguy hiểm thông qua javascript như chụp ảnh, send email, send SMS,...

+ Khuyến cáo: Cần validate dữ liệu do người dùng hoặc ứng dụng khác đưa vào để đảm bảo dữ liệu này không chứa các ký tự đặc biệt trước khi truyền cho hàm stringByEvaluatingJavaScriptFromString.

4. 3 Ngăn chặn lỗi TapJacking

- Trên Android:

+ Nguy cơ: Kẻ tấn công có thể lợi dụng giả mạo giao diện đánh lừa người dùng thực hiện một chức năng được ẩn bên dưới giao diện đó.

+ Yêu cầu: Khi định nghĩa các thành phần layout quan trọng cần thiết lập thêm thuộc tính filterTouchesWhenObscured.

Ví dụ: Định nghĩa một button buy như sau.

```
<Button android:text="Buy"
    android:id="@+id/buy"
    android:layout_width="wrap_content"
    android:layout_height="wrap_content"
    android:filterTouchesWhenObscured="true">
</Button>
```

- Trên IOS: Không tồn tại lỗi này

4. 4 Ngăn chặn lỗi khi thao tác với file

- Tránh lỗi Path Traversal.

+ Nguy cơ: Khi tên file không lọc kí tự đặc biệt dạng ”/../” thì sẽ xảy ra lỗi path traversal.

+ Yêu cầu: Với các tên file do người dùng nhập vào thì cần lọc các ký tự đặc biệt để tránh lỗi path traversal.

- Tránh lỗi đường dẫn có chứa byte null.

+ Nguy cơ: Kẻ tấn công có thể lợi dụng chèn byte null để lừa chương trình về tên file. Ví dụ: tên file là ”Documents/secret.jsp\0.jpg”, chương trình sẽ hiểu là file jpg, được phép mở hoặc upload lên server, tuy nhiên nếu chương trình không lọc các ký tự null byte thì file sẽ có định dạng như sau: ”Documents/secret.jsp”, là định dạng file không được phép thực thi.

+ Yêu cầu: Cần kiểm tra đường dẫn file, lọc null byte (%00, \0, 0x00) trước khi thao tác với file.

- Luôn kiểm tra mã trả về khi thực hiện các hàm thao tác với file.

+ Nguy cơ: Khi thao tác với các file, có thể xảy ra nhiều trường hợp như file tồn tại/không tồn tại, file đang được thay đổi, ... Điều này có thể gây ra xung đột, truy cập thay đổi các file không được phép

+ Yêu cầu: Trong quá trình thao tác với file luôn kiểm tra mã trả về khi gọi các hàm, đảm bảo thao tác đúng với file cần thao tác.

- Kiểm tra url khi gửi url sang ứng dụng khác thực thi.

+ Nguy cơ: Khi gửi url sang cho ứng dụng khác thực thi theo protocol mà ứng dụng đó đăng ký, nếu ứng dụng đó bị lỗi thì có thể tạo cầu nối tấn công, hoặc ứng dụng đó có hại thì nó có thể chuyển url sang tiếp 1 ứng dụng khác xử lý. Ví dụ như thay vì xử lý nó sẽ lừa chuyển sang trình duyệt xử lý.

+ Yêu cầu: Nên kiểm tra url trước khi gửi đi, xem có đúng định dạng nội dung mà mình muốn gửi đi hay không. Và kiểm tra xem ứng dụng nhận url có đúng là ứng dụng mình mong muốn hay không.

Ví dụ: Kiểm tra xem ứng dụng nhận url có thực sự chạy hay không, hay là chuyển sang ứng dụng khác.

Objective-C:

```
- (BOOL)application:(UIApplication *)application openURL:(NSURL
*)url          sourceApplication:(NSString *)sourceApplication
annotation:(id)annotation {
        NSString* myBid = [[NSBundle mainBundle] bundleIdentifier];
        if ([sourceApplication isEqualToString:myBid])
        {
                return NO;
        }
        ...
}
```

Swift:

```
    func application(_ application: UIApplication, open url: URL,
sourceApplication: String?, annotation: Any) -> Bool {
        if sourceApplication?.elementsEqual(myBid)
        {
            return true
        }
        ...
    }
```

Ví dụ: Kiểm tra url có đúng là được mở bằng trình duyệt Safari hay không.

Objective-C:

```
 (BOOL)application:(UIApplication *)application openURL:(NSURL
*)url  sourceApplication:(NSString *)sourceApplication
annotation:(id)annotation {
        NSString *SafariPath = @"/Applications/MobileSafari.app";
        NSBundle *bundle = [NSBundle bundleWithPath:SafariPath];
        if ([sourceApplication isEqualToString:[bundle bundleIdentifier]])
        {
                return No;
        }
        ...
}
```

Swift:

```
    func application(_ application: UIApplication, open url: URL,
sourceApplication: String?, annotation: Any) -> Bool {
        let SafariPath = "/Applications/MobileSafari.app"
        let bundle = Bundle(path: SafariPath)
        if sourceApplication?.elementsEqual(bundle?.bundleIdentifier)
        {
            return true
        }
        ...
    }
```

5. Bảo mật các thành phần của ứng dụng.

- Trên Android

+ Thiết lập quyền bảo vệ Activity

- **Nguy cơ:**

❖ Khi cần phát triển ứng dụng trong đó cung cấp cơ chế cho phép các ứng dụng khác tương tác với Activity, nếu lập trình viên sử dụng thuộc tính **android:exported=”true”** hoặc định nghĩa **intent-filter,** mà không thiết lập quyền gọi Activity này thì kẻ tấn công có thể lợi dụng xây dựng các ứng dụng xấu và gọi đến Activity này, thực hiện các hành động phá hoại, không mong muốn.

❖ Khi ứng dụng cần gọi tới một Activity của ứng dụng khác để thực hiện một hành động nào đó, mà không chỉ rõ Activity của chương trình nào, thì Android sẽ cho phép người dùng lựa chọn các ứng dụng cùng có Activity như vậy. Khi đó kẻ tấn công có thể lợi dụng tạo một Activity có cùng tên, để đánh lừa người dùng và ăn cắp thông tin ...

- **Khuyến cáo:**

❖ Đối với việc tạo Activity:

Ví dụ: Việc khai báo các tham số của Activity trong file AndroidManifest.xml như sau.

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.example.testapps.test1">
...
<activity
    android:exported="true"
    android:name=".User_login"
    android:label="@string/title_activity_main"
    android:configChanges="orientation"
    android:theme="@android:style/Theme.Black">
<intent-filter>
...
</intent-filter>
</activity>
...
</manifest>
```

Bằng việc khai báo các tham số của Activity như trên thì bất cứ ứng dụng nào cúng có thể gọi đến Activity này mà không đòi hỏi quyền gì cả. Để khắc phục điều này ta có thể khai báo như sau.

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.example.testapps.test1">
...
<permission
   android:name="com.example.testapps.test1.permission.User_login"
   android:protectionLevel="signature"
   android:label="@string/permission_label"
   android:description="@string/permission_desc">
</permission>
...
<activity
android:name=".User_login"
android:label="@string/title_activity_main"
android:configChanges="orientation"
android:theme="@android:style/Theme.Black"
android:permission="com.example.testapps.test1.permission.User_login
">
<intent-filter>
...
</intent-filter>
</activity>
...
</manifest>
```

Bằng việc khai báo như trên thì một ứng dụng nào muốn gọi Activity này thì cần phải xin quyền được định nghĩa ở trên.

Chú ý: Thuộc tính (android:protectionLevel="signature") có 4 cấp độ lựa chọn khác nhau ("normal" | "dangerous" | "signature" | "signatureOrSystem") Tùy thuộc vào mức độ bảo mật ta lựa chọn các quyền này.

- ❖ Đối với việc gọi Activity:

Ví dụ: đoạn mã chương trình gọi Activity như sau.

```
...
Intent i =  new   Intent(Intent.ACTION_DIAL);
i.setData(Uri.parse("tel:0986286086"));
startActivity(i);
...
```

Đoạn mã chương trình trên không chỉ định rõ Activity nào, vì vậy có thể bị kẻ tấn công lợi dụng tạo một chương trình và đăng ký intent-filter với dữ liệu được thiết lập là "tel" thì đoạn code trên sẽ gọi cả chương trình mà kẻ tấn công thiết lập. Khuyến cáo không gọi Activity theo kiểu này, mà cần chỉ định rõ Activity nào sẽ được gọi như ví dụ dưới đây.

```
...
intent i =  new   Intent(Intent.ACTION_VIEW);
i.setData(Uri.parse("tel:0986286086"));
i.setComponent(new ComponentName("mycontext" , "trustactivity"));
startActivity(i);
...
```

Đoạn mã chương trình trên chỉ định rõ Activity là (trustactivity) vì vậy khắc phục được vấn đề trên.

+ Thiết lập quyền cho việc gửi và nhận Broadcast

o **Nguy cơ:** Nếu không thiết lập quyền phù hợp khi đăng ký nhận broadcast kẻ tấn công có thể sử dụng Broadcast Receiver để gửi các sự kiện giả mạo đánh lừa người dùng như giả mạo sms.. Hoặc kẻ tấn công có thể lấy cắp các thông tin quan trọng được gửi qua Broadcast Receiver.

o **Khuyến cáo:**

❖ Để phòng chống thì trong trường hợp không cần thiết lập trình viên không được thiết lập thuộc tính android:export=”true” cho Broadcast Receiver.

❖ Thiết lập quyền cho việc nhận và gửi Broadcast Receiver.

Ví dụ: Đoạn code khai báo Broadcast Receiver trong file Android-Manifest.xml như sau.

```
<receiver android:enabled="true"
   android:exported="true"
   android:name="com.isecpartners.Sample"
</receiver>
```

Với việc khai báo như trên thì bất cứ ứng dụng nào cũng có thể gửi Broadcast Receiver đến mà không đòi hỏi một đặc quyền nào. Để tránh việc này ta có thể khai báo như sau.

```
<receiver android:enabled="true"
   android:name="com.isecpartners.Sample"
   android:permission="android.permission.RECEIVE_MMS">
</receiver>
```

Với việc thiết lập Receiver như trên thì nếu một ứng dụng nào đó gửi Broadcast Receiver đến mà không được cấp quyền (android.permission.RECEIVE_MMS) thì nó sẽ không nhận Broadcast này.

❖ Thiết lập việc gửi Broadcast Receiver tới những ứng dụng được cấp quyền.

Ví dụ: Khi gửi Broadcast như sau:

```
Intent i = new Intent("com.techienjoy.action.Sms");
intent.putExtra("sms", "private information");
sendBroadcast(i);
```

Bằng việc gửi Broadcast Receiver như trên thì bất cứ ứng dụng nào cũng có thể đăng ký nhận Broadcast Receiver này, như vậy nếu thông tin được gửi đi là thông tin nhạy cảm thì kẻ tấn công có thể đăng ký một Receiver để nhận được những thông tin này. Để tránh việc này ta có thể khai báo như sau.

```
Intent i = new Intent("com.techienjoy.action.Sms");
intent.putExtra("sms", "private information");
sendBroadcast(i,"android.permission.RECEIVE_MMS“);;
```

Với việc gửi Broadcast như trên thì chỉ có những ứng dụng được cấp quyền android. permission.RECEIVE_MMS mới có thể nhận được tin nhắn.

+ Thiết lập quyền bảo vệ Services

o **Nguy cơ:** Thông thường, Service thường thực hiện các nhiệm vụ xử lý những thông tin nhạy cảm, không liên quan đến giao diện người dùng như xác thực bằng username, password, đồng bộ thông tin... Nếu gọi nhầm sang Service của Malware thì sẽ bị lộ thông tin.

o **Khuyến cáo**: Thêm Permission khi định nghĩa Service và cần kiểm tra quyền của Service đấy trước khi truyền các thông tin nhạy cảm.

Ví dụ: Đoạn mã chương trình khai báo Services trong file Android-Manifest.xml như sau.

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
```

```
package="com.example.testapps.test">
...
<service android:name=".MailListenerService"
    android:enabled="true"
    android:exported="true">
   <intent-filter>
   </intent-filter>
</service>
...
</manifest>
```

Với việc khai báo như trên thì mọi ứng dụng có thể liên kết được tới Services này, để ngăn chặn điều này thì lập trình viên có thể khai báo như sau.

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.example.testapps.test">
...
<permission
   android:name="com.example.testapps.test.permission.SERVICE"
   android:protectionLevel="dangerous"
   android:label="@string/permission_label"
   android:description="@string/permission_desc">
</permission>
...
<service android:name=".MailListenerService"
   android:permission=
"com.example.testapps.test.permission.SERVICE"
   android:enabled="true">
<intent-filter>
...
</intent-filter>
</service>
...
</manifest>
```

Bằng việc khai báo như trên thì một ứng dụng nào đó muốn giao tiếp với Services này cần phải được cấp quyền "com.example.testapps.test.permission.SERVICE".

Ngoài ra trước khi liên kết đến một Services ta cần kiểm tra xem Services đó có tin cậy hay không? Bằng việc sử dụng đoạn mã chương trình sau.

```
int result = getPackageManager().checkPermission
(android.permission.BINDSERVICES, className.getPackageName());
if(PackageManager.PERMISSION_GRANTED==result)
{// do something}
```

Đoạn mã chương trình trên sẽ kiểm tra xem className.getPackageName() có được cấp quyền android.permission.BINDSERVICES hay không? Kết quả chả về đem so sánh với PackageManager.PERMISSION_GRANTED hoặc PackageManager.PERMISSI ON_DENIED để kiểm tra điều kiện. (nếu quyền được cấp thì result == PackageMana ger.PERMISSION_GRANTED, nếu không được cấp thì result == PackageManager.PER MISSION_ DENIED).

+ Bảo vệ dữ liệu nhạy cảm khi sử dụng Content Provider

o **Nguy cơ:** Content Provider cho phép định nghĩa và truy cập các dữ liệu dùng chung. Tuy nhiên, nếu việc kiểm tra quyền không được kiểm soát tốt thì người dùng có thể truy cập được các dữ liệu mà nó không được phép.

o **Khuyến cáo:** Sử dụng chính sách đặc quyền tối thiểu để phân quyền cho dữ liệu.

Ví dụ: Đoạn mã chương trình khai báo Provider trong file Android-Manifest.xml như sau:

```
<manifest
xmlns:android="http://schemas.android.com/apk/res/android"
package="com.example.testapps.test1">
...
<provider android.name="com.example.testapps.test1.MailProvider"
android.authorities="com.example.testapps.test1.mailprovider" >
</provider>
...
</manifest>
```

Với việc khai báo Provider như trên thì bất cứ ứng dụng nào cũng có thể truy cập tới Provider này và có thể thêm sửa xóa dữ liệu trong Provider này. Để thiết lập quyền bảo mật cho Provider ta có thể cấu hình như sau:

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.example.testapps.test1">
...
<permission
  android:name="com.example.testapps.test1.permission.DB_READ"
  android:protectionLevel="dangerous"
...
</permission>
<permission
  android:name="com.example.testapps.test1.permission.DB_WRITE"
  android:protectionLevel="dangerous"
...
</permission>
...
<provider android.name="com.example.testapps.test1.MailProvider"
android.authorities="com.example.testapps.test1.mailprovider"
android.readPermission="com.example.testapps.test1.permission.DB_READ"
android.writePermission="com.example.testapps.test1.permission.DB_WRITE">
<grant-uri-permission android:path="/attachments/" />
</provider>
...
</manifest>
```

Với việc thiết lập quyền như trên thì những ứng dụng nào xin quyền đọc hoặc ghi thì mới có thể đọc hoặc ghi được Provider này, trong trường hợp khai báo trên thì khi các ứng dụng được cấp quyền chỉ có thể đọc hoặc ghi giới hạn trong thư mục (/attachments).

- Trên iOS:

+ Lỗi buffer overflow

o **Nguy cơ:** Lỗi tràn bộ đệm có thể cho phép kẻ xấu chèn vào mã độc thực hiện hành vi xấu trong chương trình.

o **Yêu cầu:**

❖ Kiểm tra dữ liệu đầu vào

❖ Dùng các hàm thao tác buffer của Objective-C, hạn chế sử dụng các hàm của C. Nếu phải dùng thì nên dùng các hàm an toàn như bảng sau.

❖ Bảng các hàm C thao tác với buffer an toàn.

Không nền dùng	Nên dùng để thay thế
strcat	strlcat
strcpy	strlcpy
strncat	strlcat
strncpy	strlcpy
sprintf	snprintf or asprintf
vsprintf	vsnprintf or vasprintf
gets	fgets

+ Lỗi format string

o **Nguy cơ:** Khi thao tác với xâu, kẻ tấn công có thể đưa các ký tự đặc biệt sử dụng trong để định dạng xâu như ”%n”, ”%@”, ... vào trong xâu gốc, để chương trình nhầm lẫn trong thực thi, đọc sang các dữ liệu không mong muốn.

o **Yêu cầu:**

❖ Kiểm tra dữ liệu đầu vào.

❖ Đặc biệt chú ý khi sử dụng NSLog để ghi log, vì NSLog có format string, mà lập trình viên thường không chú ý kiểm soát dữ liệu log.

+ Lỗi sử dụng bộ nhớ sau khi đã giải phóng

o **Nguy cơ:** Trong nhiều ứng dụng, xảy ra trường hợp sử dụng 1 biến đã giải phóng trước đó gây ra lỗi bộ nhớ, có thể gây crash cho ứng dụng và kẻ tấn công có thể lợi dụng lỗi này để kết hợp với lỗi khác để tấn công ứng dụng.

o **Khuyến cáo:**

❖ Tùy chọn biên dịch an toàn

❖ Nên kiểm tra các đối tượng trước khi sử dụng, tránh sử dụng đối tượng đã giải phóng

6. Lập trình an toàn với thông tin Logs và Debuger

- Trên Android:

+ Không được ghi logs các thông tin người dùng

- Nguy cơ: Khi lập trình, debug ứng dụng, lập trình viên thường tiến hành ghi log hoặc đặt một số thông tin debug có thể làm lộ thông tin nhạy cảm.

Ví dụ: Đoạn chương trình ghi logs như sau.

```
try {
    userInfo = client.validateCredentials(userName, password);
    if (userInfo.get("success").equals("true"))
        launchHome(v);
    else {
        Log.w("Failed login", userName + " " + password);
    }

} catch (Exception e) {
    Log.w("Failed login", userName + " " + password);
}
```

Với việc ghi logs như trên thì sẽ logging lại cả thông tin về tên đăng nhập và mật khẩu của người dùng khi đăng nhập không thành công. Như vậy sẽ để lộ thông tin về tên đăng nhập và mật khẩu của người dùng.

- **Yêu cầu:** Để tránh điều này các thông tin logs không được ghi lại các thông tin quan trọng của người dùng (password...)

+ Tắt chế độ debug

- **Yêu cầu:** Thiết lập thuộc tính <application android:debuggable="false"/> trong file androidmanifest.xml.

7. Bảo vệ mã nguồn của chương trình

- Trên Android:

+ Không hardcode các thông tin quan trọng như (keys, username/password...)

- **Nguy cơ:** Nếu lập trình viên hardcode các thông tin quan trọng như keys, username/password thì kẻ tấn công có thể dịch ngược (reverse) chương trình để lấy được những thông tin này.

- **Yêu cầu:** Thực hiện không hardcode các thông tin username/password trong mã nguồn ứng dụng.

+ Sử dụng kỹ thuật làm nhiễu mã nguồn của chương trình (obfuscate code)

- **Nguy cơ:** Khi chương trình không được làm nhiễu kẻ tấn công có thể dễ dàng dịch ngược chương trình, phân tích chức năng của chương trình, phân tích lỗi và khai thác chương trình ứng dụng.

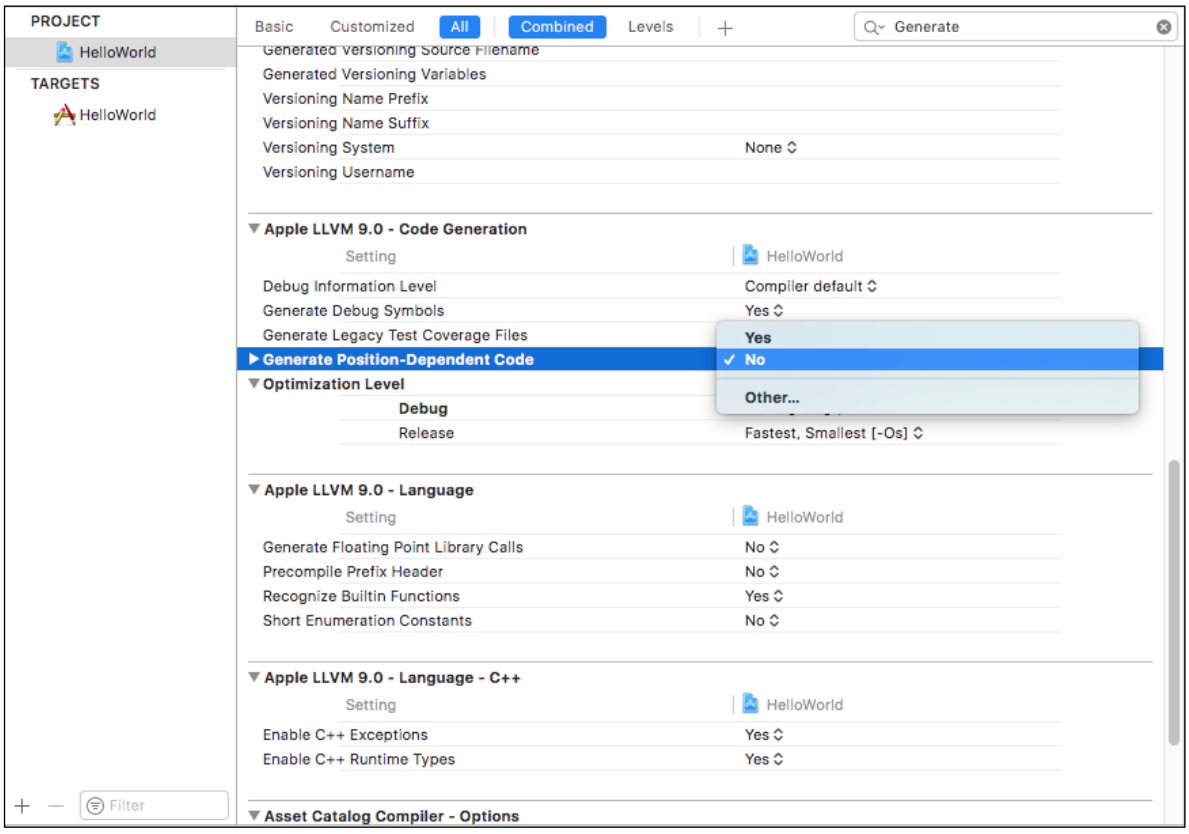
- **Khuyến cáo:** Sử dụng các chương trình như ProGuard để làm nhiễu mã nguồn của chương trình.

- Trên IOS:

+ Biên dịch với lựa chọn No cho tùy chọn Generate Position-Dependent Code

o **Nguy cơ:** Chương trình biên dịch với tùy chọn Generate Position-Dependent Code làm cho kẻ tấn công có thể xác định được địa chỉ chương trình nạp trên bộ nhớ, làm cho quá trình tấn công vào bộ nhớ chương trình dễ thành công hơn.

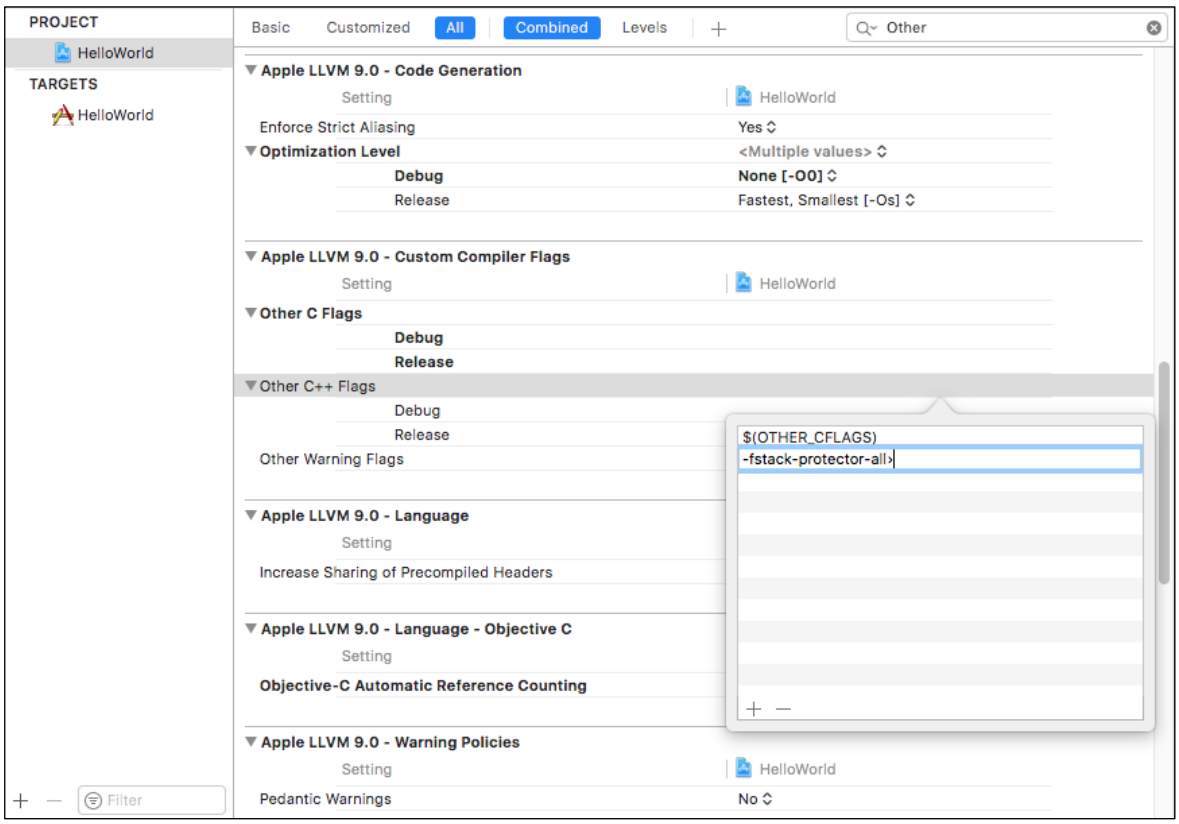
o **Khuyến cáo:** Tắt tùy chọn Generate Position-Dependent Code trong build setting của project trên Xcode (mặc định đã disable) như hình minh họa sau:



+ Biên dịch với tùy chọn bảo vệ tấn công vào ngăn xếp.

o **Nguy cơ:** Ngăn xếp không được bảo vệ sẽ không ngăn chặn kẻ tấn công chèn mã thực thi vào trong ngăn xếp khi khai thác các lỗi tràn bộ đệm dạng ngăn xếp (stack overflow).

o **Khuyến cáo:** Thêm cờ biên dịch -fstack-protector-all trong Build Setting của project.



+ Biên dịch với tùy chọn tự động đếm số tham chiếu trong quản lý bộ nhớ nhằm giảm nguy cơ chương trình gây lỗi bộ nhớ.

o **Nguy cơ:** Trong nhiều ứng dụng, xảy ra trường hợp sử dụng 1 biến đã giải phóng trước đó gây ra lỗi bộ nhớ, có thể gây crash cho ứng dụng và kẻ tấn công có thể lợi dụng lỗi này để kết hợp với lỗi khác để tấn công ứng dụng.

o **Khuyến cáo:** Chọn lựa chọn Yes cho tùy chọn Objective-C Automatic Reference Counting như hình sau:

Phụ lục 05.
HƯỚNG DẪN THIẾT LẬP CHÍNH SÁCH BẢO MẬT HĐH WINDOWS SERVER 2012

1. Cài đặt hệ điều hành và cập nhật bản vá.

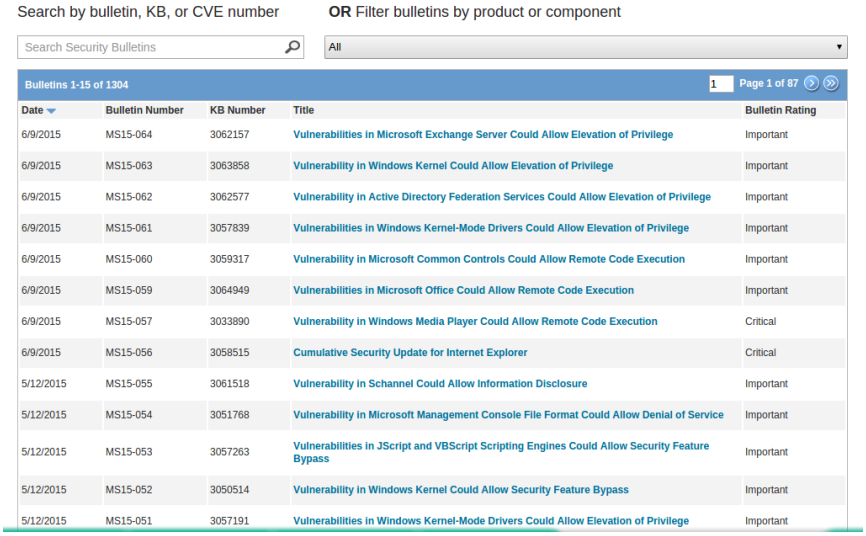
Khi tiến hành cài đặt một hệ điều hành, một trong những yêu cầu đầu tiên phải thực hiện đó là cài đặt các bản vá hoặc upgrade version mới nhất nhằm tránh các lỗ hổng về bảo mật đã tồn tại trong các phiên bản cũ.

- Đối với hệ điều hành Windows Server 2012 yêu cầu cài đặt phiên bản Windows Server 2012 R2 và cập nhật rollups mới nhất từ Microsoft.

- Hệ điều hành phải được cập nhật các bản vá security đã được Tập đoàn cảnh báo.

- Truy cập trang: https://technet.microsoft.com/en-us/security/bulletin/

Thực hiện cập nhật bản vá security mới nhất từ nhà phát triển cho hệ điều hành Windows Server tại đây.



Search by bulletin, KB, or CVE number **OR** Filter bulletins by product or component

Search Security Bulletins | All

Bulletins 1-15 of 1304 | 1 | Page 1 of 87

Date	Bulletin Number	KB Number	Title	Bulletin Rating
6/9/2015	MS15-064	3062157	Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege	Important
6/9/2015	MS15-063	3063858	Vulnerability in Windows Kernel Could Allow Elevation of Privilege	Important
6/9/2015	MS15-062	3062577	Vulnerability in Active Directory Federation Services Could Allow Elevation of Privilege	Important
6/9/2015	MS15-061	3057839	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	Important
6/9/2015	MS15-060	3059317	Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution	Important
6/9/2015	MS15-059	3064949	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution	Important
6/9/2015	MS15-057	3033890	Vulnerability in Windows Media Player Could Allow Remote Code Execution	Critical
6/9/2015	MS15-056	3058515	Cumulative Security Update for Internet Explorer	Critical
5/12/2015	MS15-055	3061518	Vulnerability in Schannel Could Allow Information Disclosure	Important
5/12/2015	MS15-054	3051768	Vulnerability in Microsoft Management Console File Format Could Allow Denial of Service	Important
5/12/2015	MS15-053	3057263	Vulnerabilities in JScript and VBScript Scripting Engines Could Allow Security Feature Bypass	Important
5/12/2015	MS15-052	3050514	Vulnerability in Windows Kernel Could Allow Security Feature Bypass	Important
5/12/2015	MS15-051	3057191	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	Important

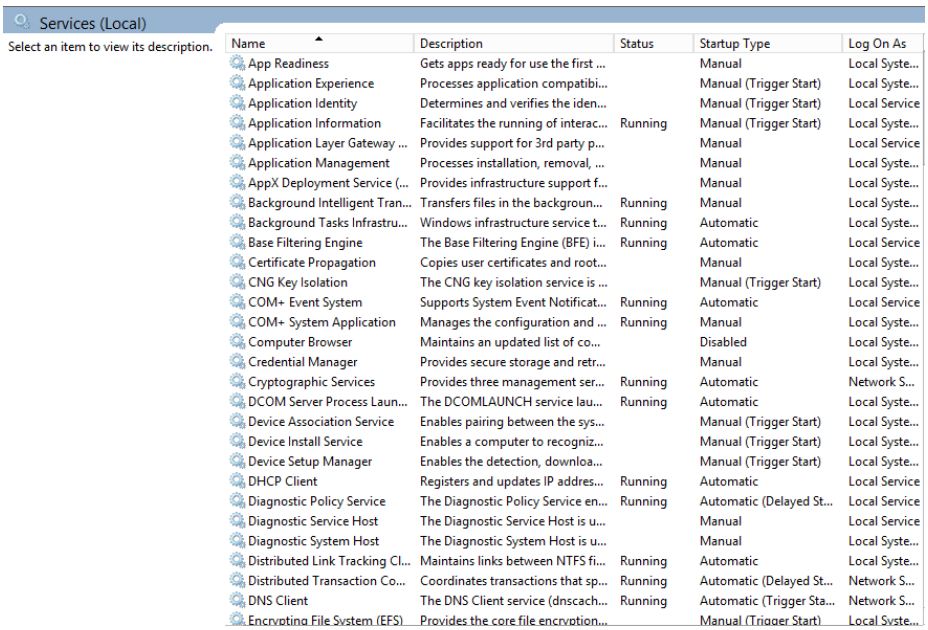
Lưu ý: Phải tiến hành thử nghiệm trên hệ thống giả lập trước khi cập nhập bản vá và phải kiểm tra các lại dịch vụ của máy chủ sau khi thực hiện nâng cấp.

2. Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết.

Trong thực tế, mỗi server (máy chủ) trong hệ thống sẽ đảm nhiệm một chức năng riêng biệt. Khi cài đặt hệ điều hành cho máy chủ, cần xóa hoặc disable tất cả các dịch vụ, ứng dụng, giao thức không cần thiết.

- Bước 1: Click vào biểu tượng cửa sổ bên trái, phía dưới của màn hình => chọn **Administrative Tools => Services.**

- Bước 2: Tìm và disable các dịch vụ không cần thiết.



Thông thường, một số dịch vụ, ứng dụng, giao thức sau nên được xóa hoặc disable nếu không sử dụng:

- Dịch vụ chia sẻ file và printer: NFS, FTP, NetBios,..

- Wireless networking.

- Chương trình hỗ trợ remote control hoặc remote access không an toàn: telnet.

- Directory services: LDAP, NIS.

- Webserver, webservices.

- Email services: smtp.

- Language compilers, libraries.

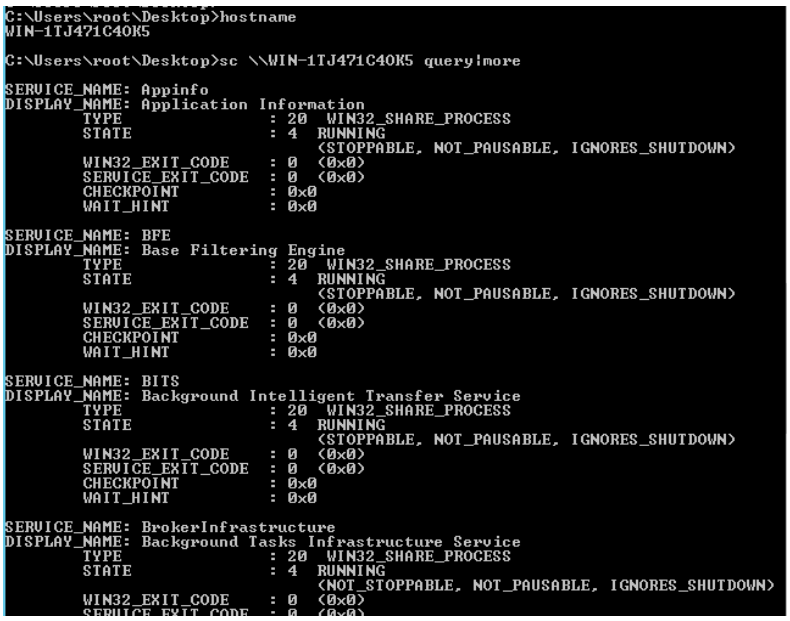
- System development tools.

- System and network management tools and utilities: SNMP.

Trường hợp sử dụng command line:

- Bước 1: Sử dụng lệnh hostname để lấy ra tên máy

- Bước 2: Sử dụng lệnh sc \\<hostname> query để lấy ra danh sách trạng thái các service.



3. Thiết lập chính sách tài khoản.

Các tài khoản mặc định của hệ thống, các tài khoản dễ đoán thường là mục tiêu tấn công, dò quét của các attacker. Mặc định hệ thống thường cung cấp các tài khoản như tài khoản guest, administrator,...với những mật khẩu mặc định.

- Xóa hoặc vô hiệu hóa các tài khoản không sử dụng trên hệ thống:

+ Kiểm tra tài khoản trên Local:

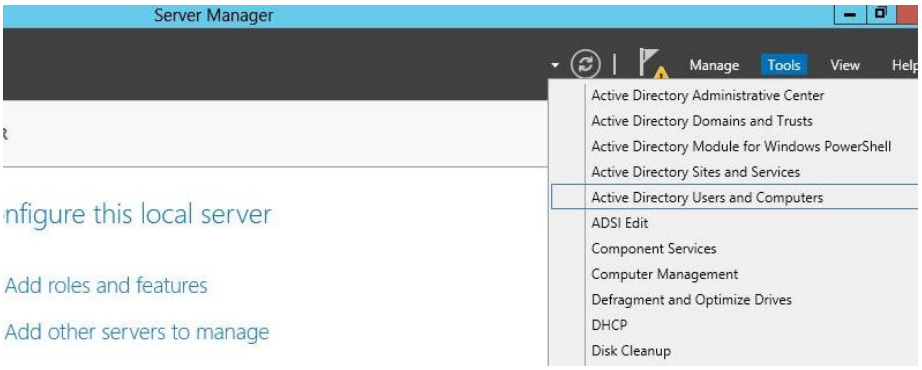
  - Bước 1: Click vào => Server Manager => Tools => Computer management => Local User and group => Users/Groups.
  - Bước 2: Kiểm tra user nào không sử dụng xóa hoặc disable.

Cách kiểm tra bằng command line:

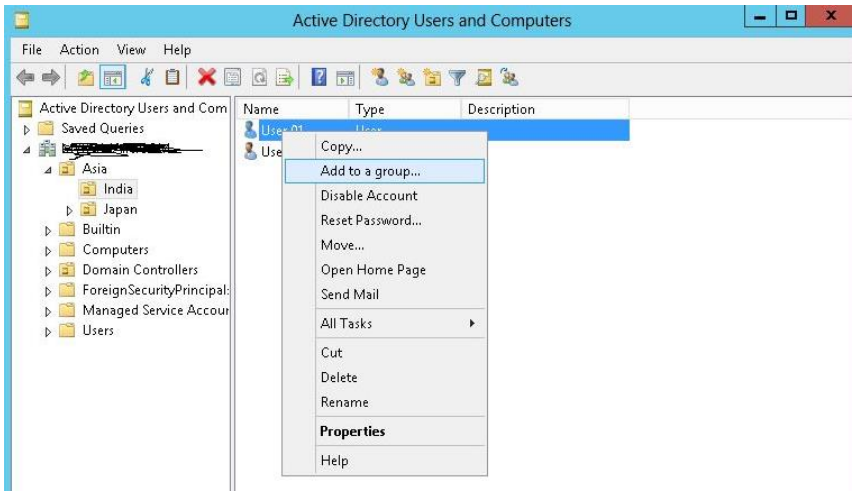
  - Bước 1: chạy lệnh net users để lấy danh sách username
  - Bước 2: chạy lệnh net user <username> để lấy thông tin về account đó, trong đó có thông tin về trạng thái active/disable của user.

```
C:\Users\root\Desktop>net users

User accounts for \\WIN-1TJ471C4OK5

-------------------------------------------------------------------------------
Administrator            Guest                    root
The command completed successfully.


C:\Users\root\Desktop>net user root
User name                    root
Full Name
Comment
User's comment
Country/region code          001 (United States)
Account active               Yes
Account expires              Never

Password last set            7/11/2016 10:39:19 AM
Password expires             Never
Password changeable          7/11/2016 10:39:19 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   7/11/2016 10:46:58 AM

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.
```

+ Kiểm tra tài khoản trên máy domain controller:
    - Bước 1: Click vào => Server Manager => Tools => Active Directory Users and Computers.



    - Bước 2: Click vào User/Group. Xóa hoặc disable tài khoản không sử dụng.



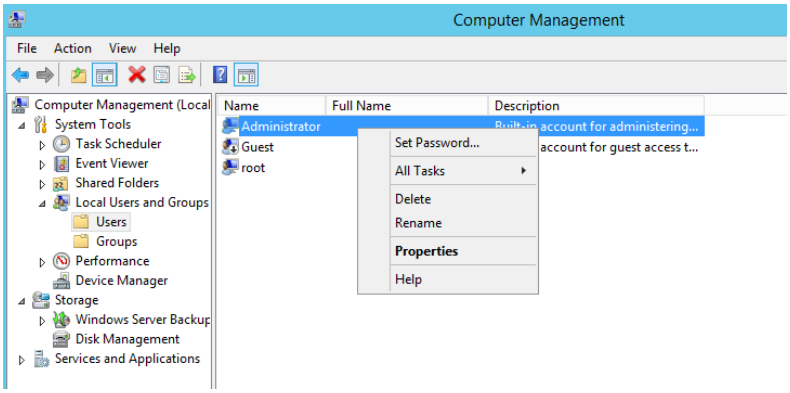
Cách kiểm tra bằng command line:

- Bước 1: chạy lệnh net users để lấy danh sách username

- Bước 2: chạy lệnh net user <username> /<domain> để lấy thông tin trên domain của account đó, trong đó có thông tin về trạng thái active/disable của user.

- Thay đổi tên, mật khẩu cho các tài khoản mặc định.

+ Thay đổi user, password trên máy Local: Click vào => Server Manager => Tools => Computer management => Local User and group => Users/Groups. Thực hiện thay đổi tên, mật khẩu cho các tài khoản mặc định. Ví dụ như: Administrator.



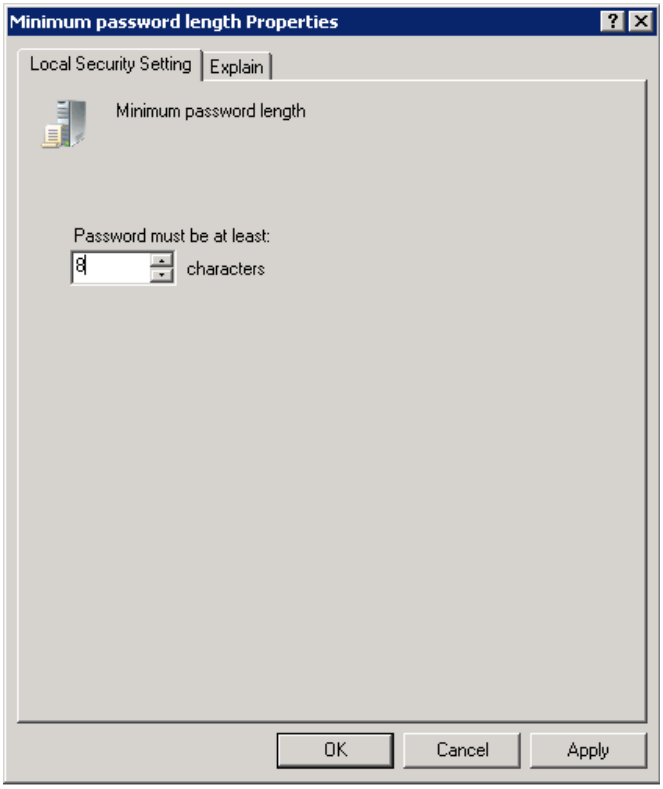
+ Thay đổi tên, mật khẩu trên máy Domain Controller:

- Bước 1: Click vào => Server Manager => Tools => Active Directory Users and Computers.
- Bước 2: Chọn tài khoản muốn thay đổi => Properties => Account. Thay đổi tên, mật khẩu của các tài khoản mặc định.

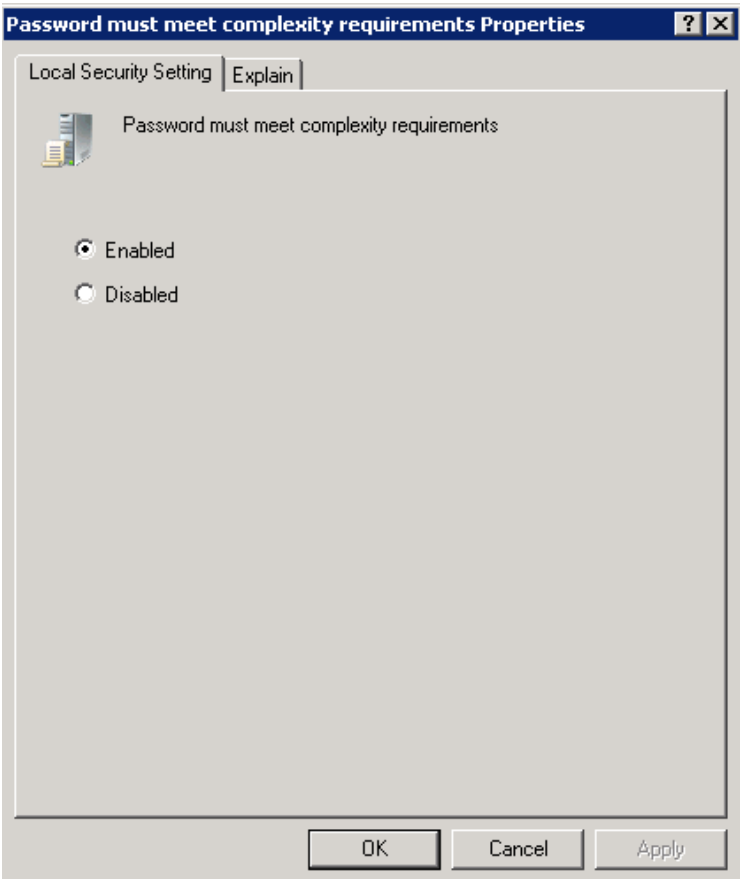
- Cấu hình chính sách mật khẩu cho tài khoản:

+ Độ dài tối thiểu của mật khẩu phải lớn hơn hoặc bằng 10 ký tự.

- Bước 1: Click chuột phải vào biểu tượng => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
- Bước 2: Chọn *Minimum Password length* và đặt 10 ký tự.



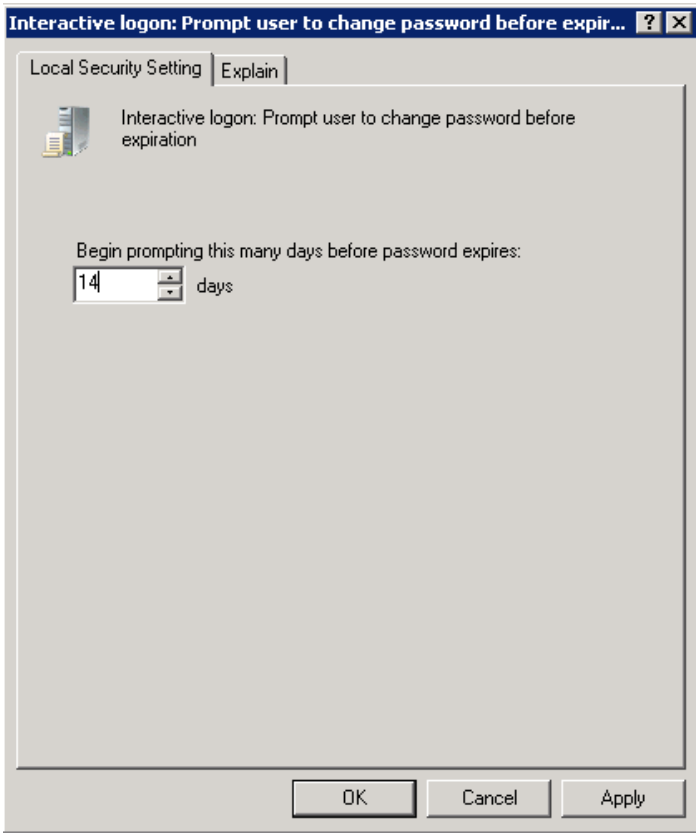
+ Mật khẩu phải chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt.
    - Bước 1: Click chuột phải vào biểu tượng > Administrative Tools => Local Security Policy => Account Policies => Password Policy.
    - Bước 2: Chọn *Password must meet complexity* và tick vào Enabled.



+ Thời gian bắt buộc phải thay đổi mật khẩu.

  - Bước 1: Click chuột phải vào biểu tượng => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
  - Bước 2: Chọn *Maximum Password Age* và đặt 90 ngày (với hệ thống public) hoặc 180 ngày (với hệ thống nội bộ).

  - Bước 3: Cấu hình thông báo mật khẩu sắp hết hạn cho người dùng. Click chuột phải vào biểu tượng => Administrative Tools => Local Security Policy => Local Policies => Security Options. Thiết lập giá trị cho cấu hình *Interactive logon: Prompt user to change password before expire* là 14.



+ Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất.

  - Bước 1: Click chuột phải vào biểu tượng => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
  - Bước 2: Chọn *Enforce password history* và đặt giá trị là 02 (với hệ thống nội bộ) hoặc 05 (với hệ thống public).

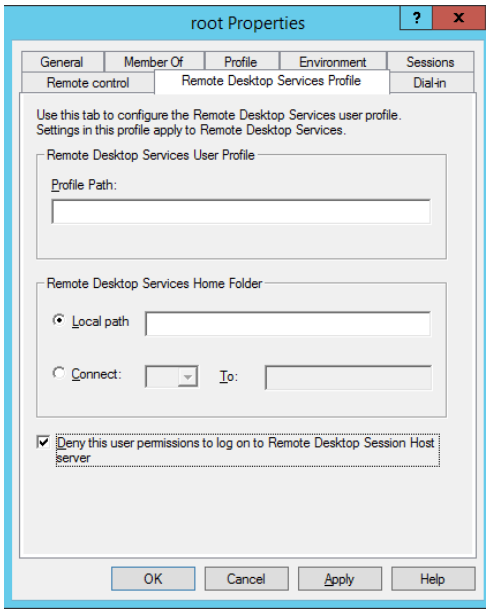
4. Quản trị từ xa qua kênh truyền an toàn.

- Yêu cầu quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa: Sử dụng ứng dụng Remote Desktop của Windows để quản trị từ xa.

- Cấu hình giới hạn tài khoản được phép sử dụng dịch vụ quản trị từ xa.

+ Bước 1: Click vào => Server Manager => Tools => Computer management => Local User and group => Users

+ Bước 2: Click chuột phải vào user không được phép sử dụng quản trị từ xa chọn Properties, chọn phần Remote Desktop Service Profile, tick chọn vào checkbox "Deny this user permissions to log on Remote Desktop Session Host server" để chặn user logon từ xa. Việc chặn được thực thi ngay lập tức, không cần khởi động lại dịch vụ.



- Giới hạn số lần đăng nhập sai là 05 lần.

+ Bước 1: Click chuột phải vào biểu tượng => Administrative Tools => Local Security Policy => Account Policies => Password Policy.

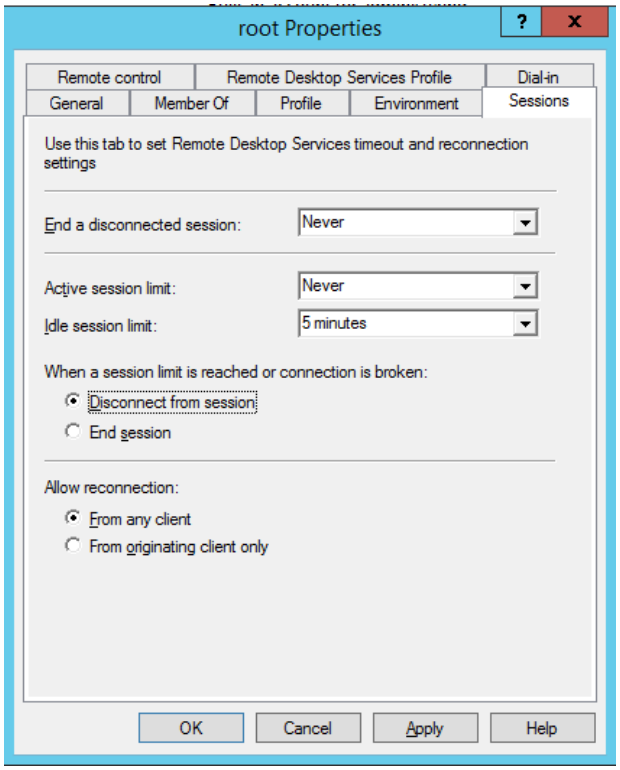
+ Bước 2: Chọn *Account lockout threshold* và thiết lập giá trị là 5, *Account lockout duration* thiết lập là 5 và *Reset account lockout counter after* thiết lập giá trị là 5.

Policy	Security Setting
Account lockout duration	5 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	5 minutes

- Giới hạn thời gian tự động ngắt phiên khi không có hoạt động trong một khoảng thời gian là 5 phút.

+ Vào => Server Manager => Tools => Computer management => Local User and group => Users.

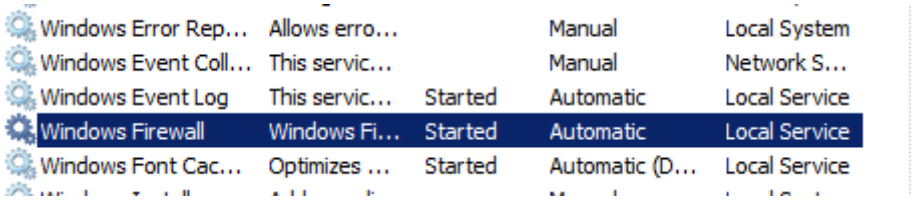
+ Click chuột phải vào user không được phép sử dụng quản trị từ xa chọn Properties, chọn phần Remote Desktop Service Profile, tick chọn 5 minutes cho giá trị Idle Session limit.



5. Cài đặt và cấu hình firewall mềm.

Trên một server luôn có rất nhiều các dịch vụ đang chạy đồng thời, việc kiểm soát tất cả mọi truy cập vào ra trên hệ thống sẽ giúp hạn chế được các cuộc tấn công của attacker.

- Kích hoạt Windows Firewall: Run => services.msc => Chọn Windows Firewall => Chọn Automatic => Start.



- Mặc định Windows Firewall cấm các kết nối vào và không cấm các kết nối ra đối với cả Domain Profile, Private Profile và Public Profile:

+ Domain Profile: Cấu hình tường lửa được áp dụng khi máy tính kết nối với các máy khác trong cùng một domain.

+ Private Profile: Cấu hình tường lửa được áp dụng khi máy tính kết nối với mạng riêng.

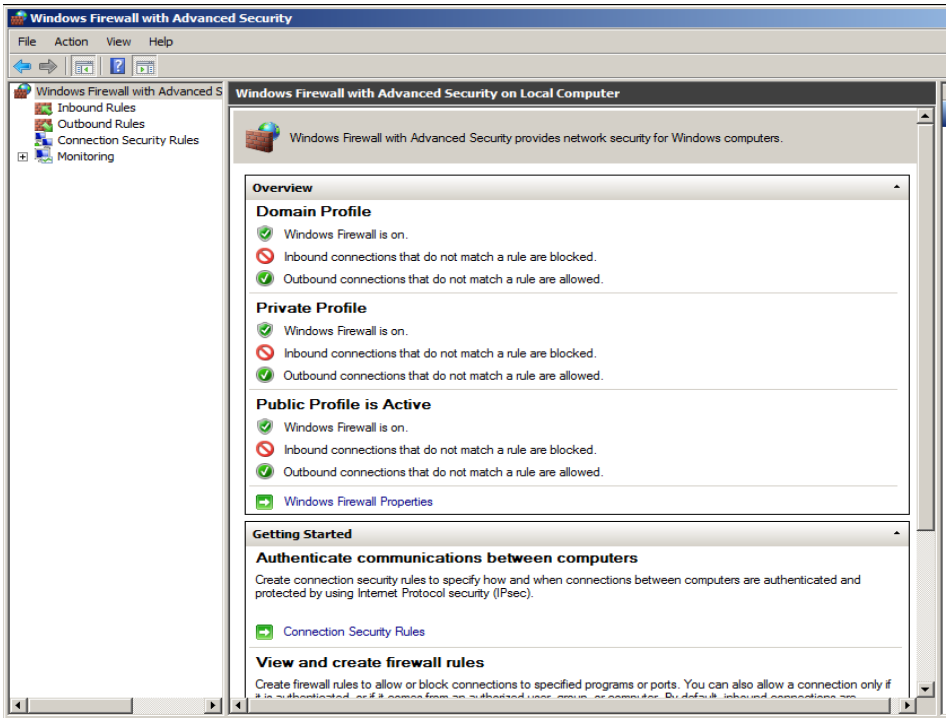
+ Public Profile: Cấu hình tường lửa được áp dụng khi máy tính kết nối với mạng công cộng.

+ Local IP: là địa chỉ trên máy chủ đang chấp nhận kết nối hoặc địa chỉ được sử dụng với tư cách là địa chỉ nguồn để gửi các kết nối gửi đi.

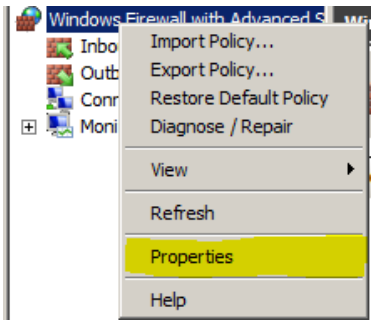
+ Remote IP: là địa chỉ IP của máy chủ điều khiển xa mà máy chủ này đang muốn kết nối đến (trong kịch bản truy cập gửi đi), hoặc địa chỉ IP nguồn của máy tính đang muốn kết nối với máy chủ (trong trường hợp kịch bản truy cập gửi đến).

+ Local Port: các cổng nội bộ trên máy chủ mà rule của tường lửa sử dụng. Nếu rule là Inbound Rules thì đây sẽ là cổng để máy chủ lắng nghe. Nếu rule là Outbound Rules thì đây sẽ là cổng nguồn để máy chủ sử dụng kết nối tới máy khác.

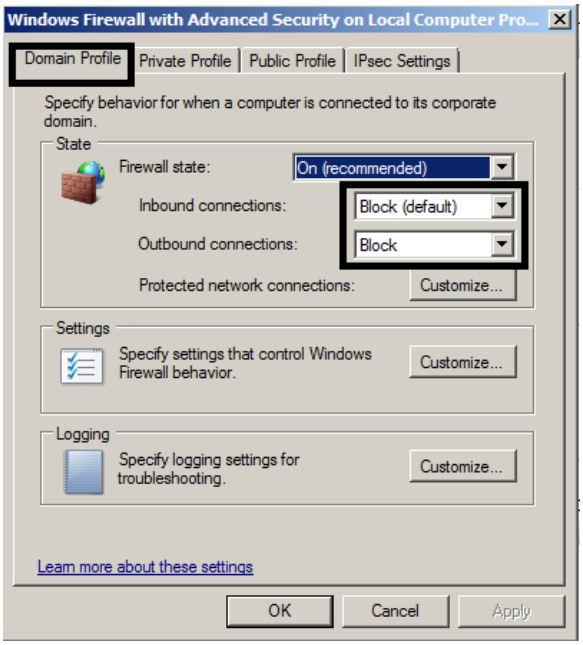
+ Remote Port: đây là cổng điều khiển từ xa để sử dụng cho rule. Trong trường hợp rule kết nối gửi đi thì đây sẽ là cổng mà máy chủ kết nối với một máy tính khác. Trong trường hợp rule kết nối đến thì đây chính là cổng nguồn của máy tính muốn kết nối với máy chủ.



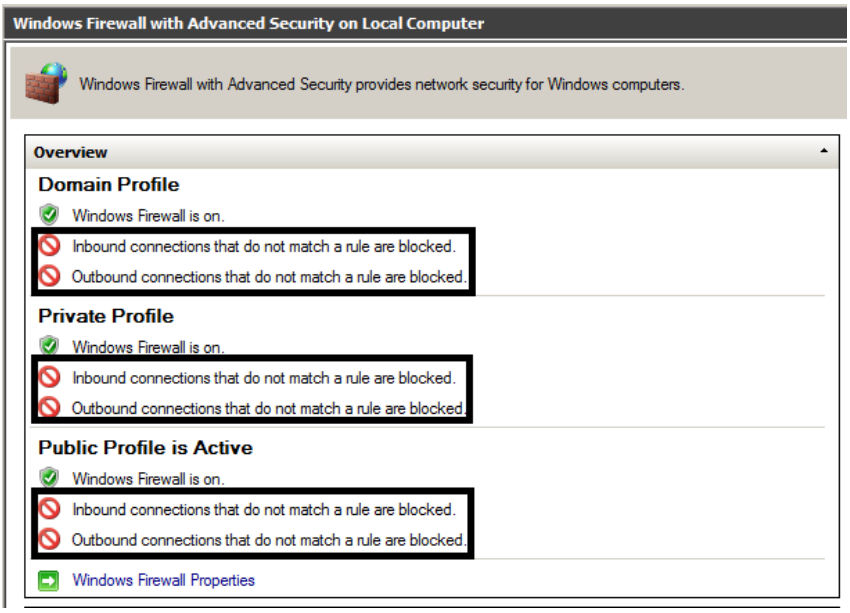
- Cấu hình block các kết nối ra ngoài:



+ Cấu hình Block Outbound Connection trong tab Domain Profile (làm tương tự đối với tab Private Profile và Public Profile).

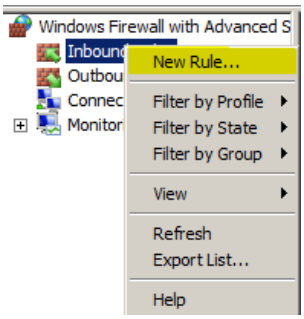


+ Kiểm tra lại cấu hình xem đã được kích hoạt chưa:

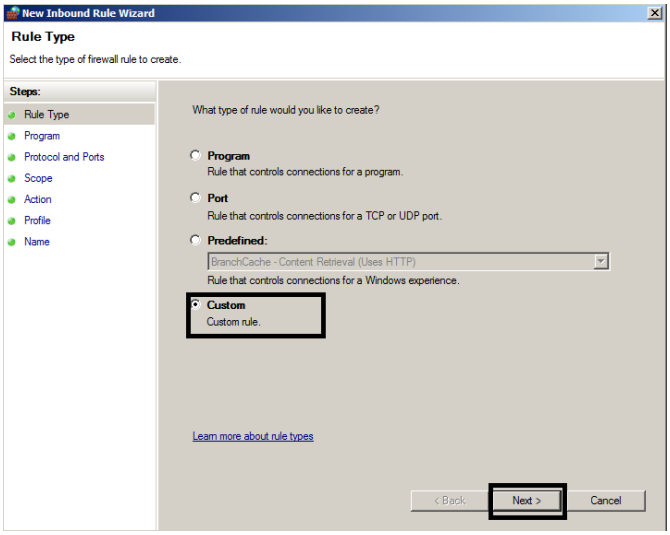


- Thiết lập kết nối chiều ra/vào theo đặc quyền:

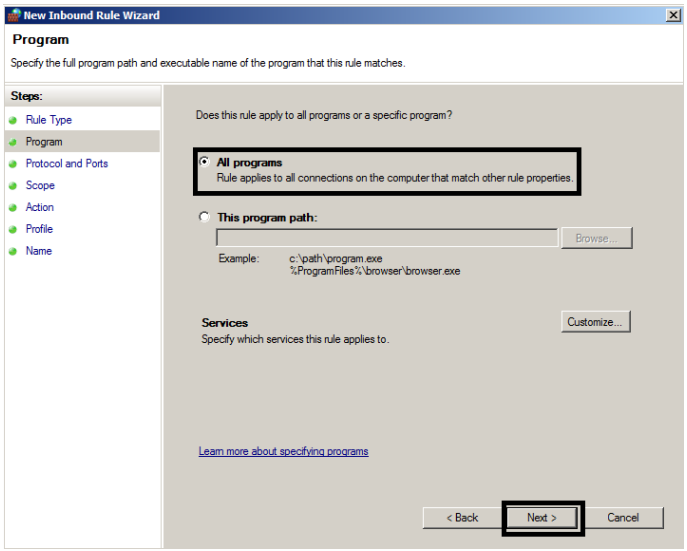
+ Thiết lập chính sách kết nối từ ngoài vào máy chủ (Inbound Rule): Click chọn Inbound Rule => New Rule…



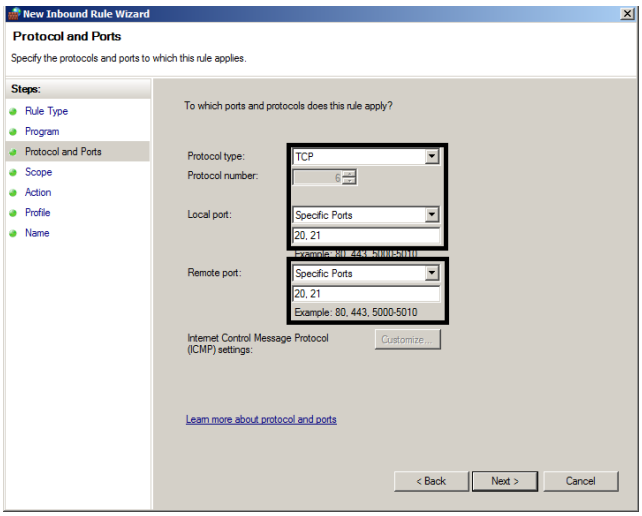
+ Chọn Custom và click Next:



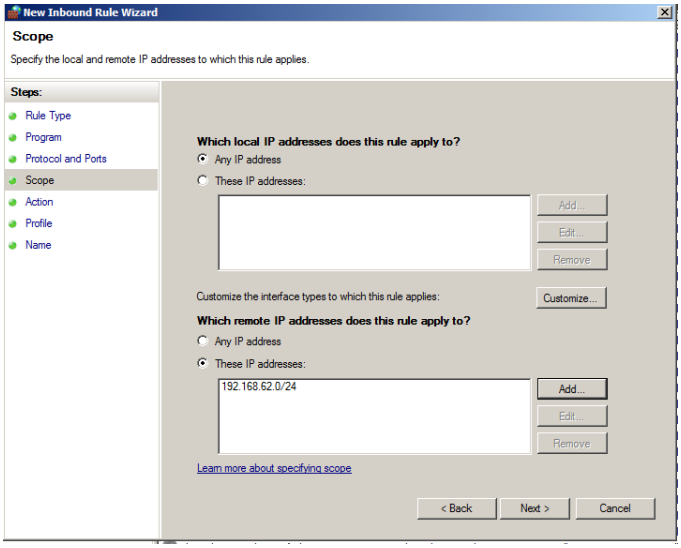
+ Chọn chương trình kết nối => All Programs => Next.



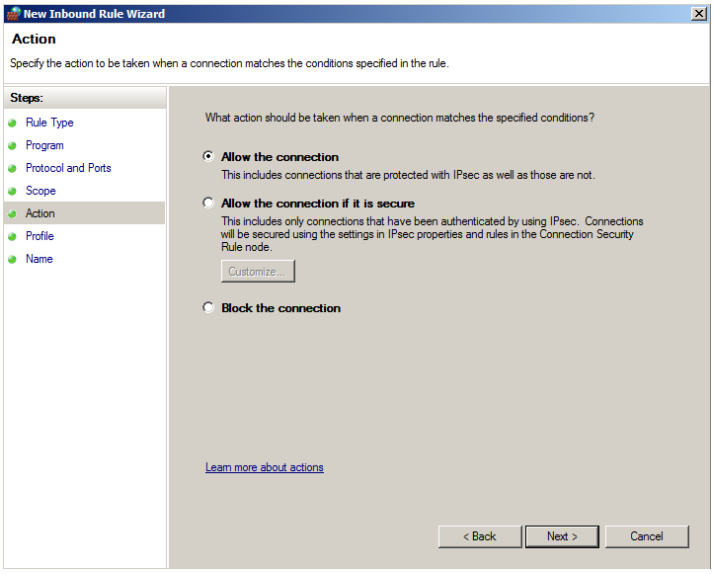
+ Chọn giao thức và cổng tương ứng cần mở kết nối từ ngoài vào máy chủ. Ví dụ chọn giao thức TCP, cổng 20, 21 => Click Next.



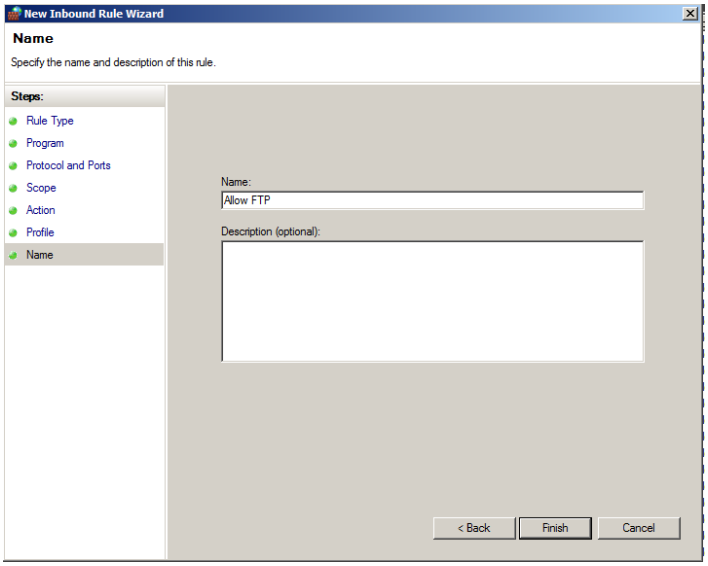
+ Thiết lập IP được phép kết nối => Click Next:



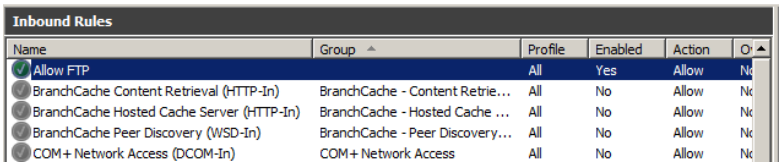
+ Chọn Allow the connection => Click Next:



+ Để mặc định => Next => Đặt tên cho Rule => Click Finish:



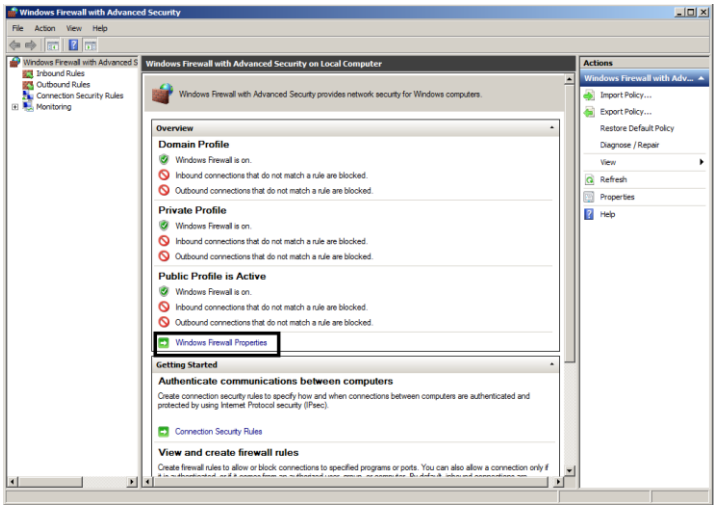
+ Ta có được luật vừa tạo:



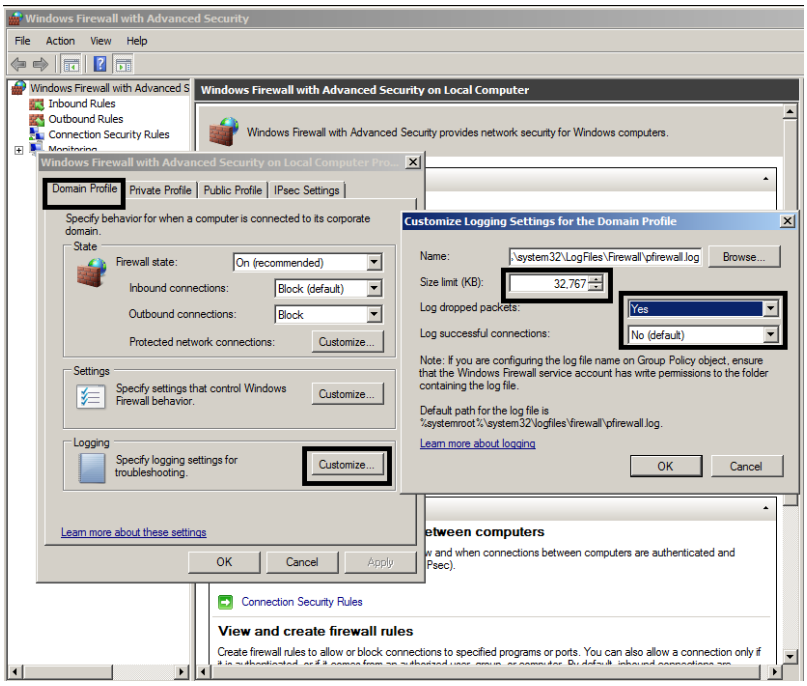
+ Thiết lập chính sách kết nối từ máy chủ ra ngoài (Outbound Rule): Cách thiết lập tương tự như trên.

- Yêu cầu ghi log toàn bộ các gói tin vi phạm luật tường lửa.

+ Vào Start => Administrative Tools => Windows Firewall with Advanced Security.



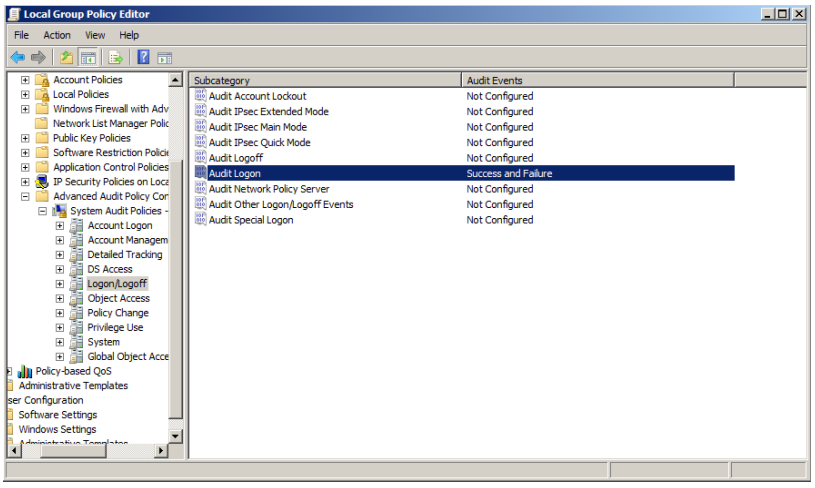
+ Click Windows Firewall Properties => mở Customize… Logging của các tab Domain Profile, Private Profile và Public Profile => Click Yes cho Log dropped packets.



6. Thiết lập chính sách quản lý log.

- Ghi log các sự kiện đăng nhập vào máy chủ.

+ Vào Run => gpedit.msc => Computer Configuration => Windows Setting => Security Setting => Advanced Audit Policy Configuration => System Audit Policy – Local Group Policy Object => Logon/logoff => Audit Logon => Configure the following audit event => Chọn Failure và Success.

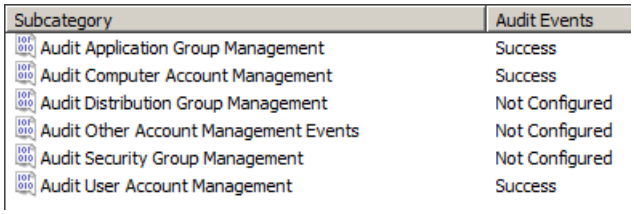


- Ghi log các sự kiện liên quan đến quản lý tài khoản và nhóm tài khoản.

+ Vào Run => gpedit.msc => Computer Configuration => Windows Setting => Security Setting => Advanced Audit Policy Configuration => System Audit Policy – Local Group Policy Object => Account Management.

+ Cấu hình như sau:

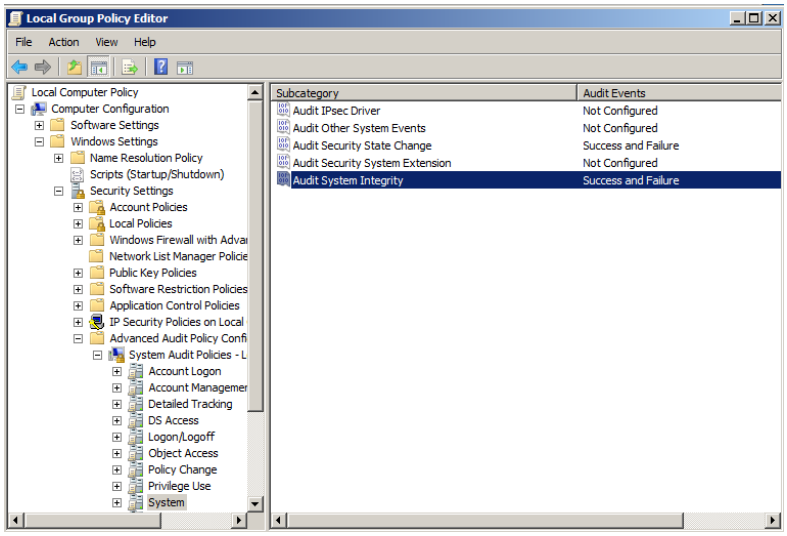
- Audit Application Group Management => Chọn Success.
- Audit Computer Account Management => Chọn Success.
- Audit User Account Management => Chọn Success.



- Ghi log những thay đổi trong "Security State Change" và "System Integrity".

+ Vào Run => gpedit.msc => Computer Configuration => Windows Setting => Security Setting => Advanced Audit Policy Configuration => System Audit Policy – Local Group Policy Object => System:

- Audit Security State Change => Chọn Failure và Success.
- Audit System Integrity => Chọn Failure và Success.

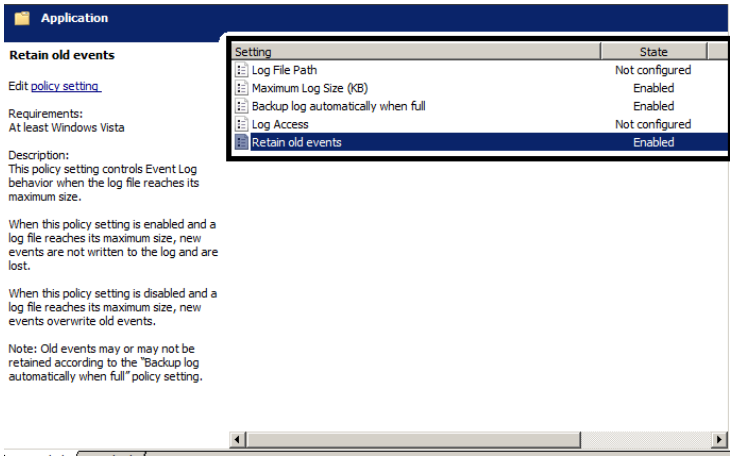


- Thiết lập kích cỡ và sao lưu file log Application, Security, System.

+ Vào Run => gpedit.msc => Computer Configuration => Administrative Templates => Windows Components => Event Log Service. Đối với cả 3 mục Application, Security, System thiết lập như sau:

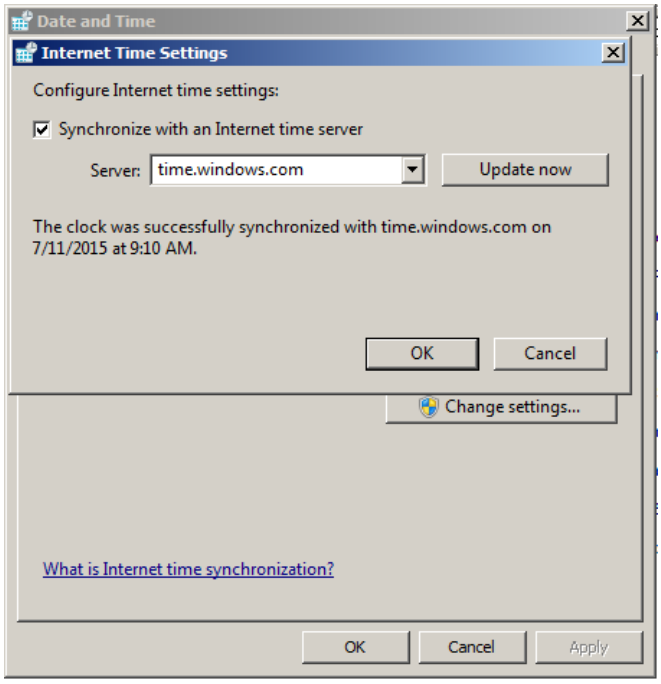
- Application => Maximum Log Size (KB) thiết lập kích cỡ 1024000 KB.
- Security => Maximum Log Size (KB) thiết lập kích cỡ 1024000 KB.
- System => Maximum Log Size (KB) thiết lập kích cỡ 1024000 KB.

- Bật: Backup log automatically when full.



- Cấu hình đồng bộ thời gian cho hệ thống:

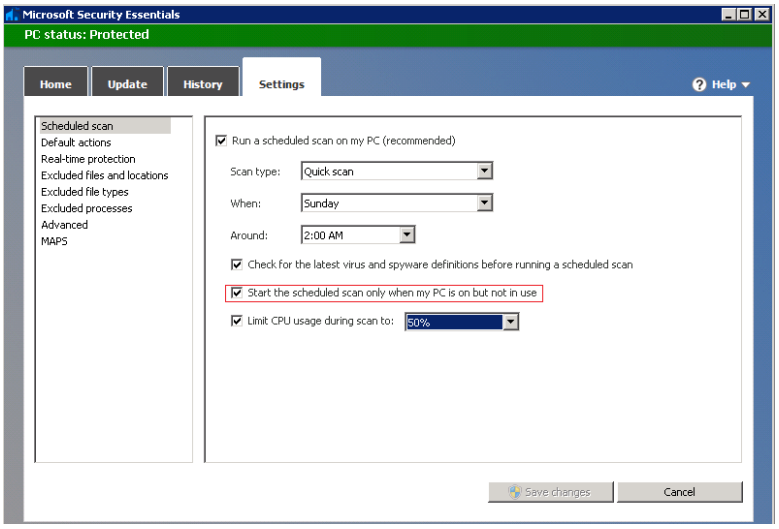
+ Click vào biểu tượng thời gian Date and Time => Internet Time => Change Setting => chọn "Synchronize with an Internet Time Server" => nhập địa chỉ Time Server => Update now.



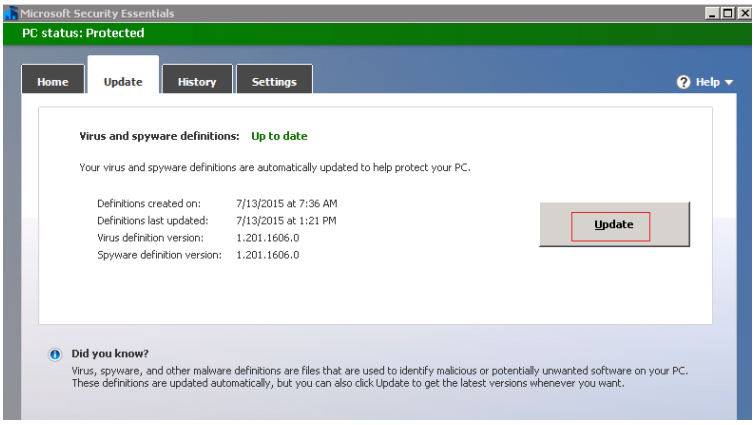
7. Cài đặt phần mềm diệt virus.

Yêu cầu cài đặt các phần mềm antiVirus nhằm ngăn ngừa, phát hiện các cuộc tấn công của attacker vào hệ thống. Trong phần này, phụ lục chi tiết hướng dẫn cấu hình phần mềm diệt virus Microsoft Security Essentials (MSE) theo các đầu mục của baseline.

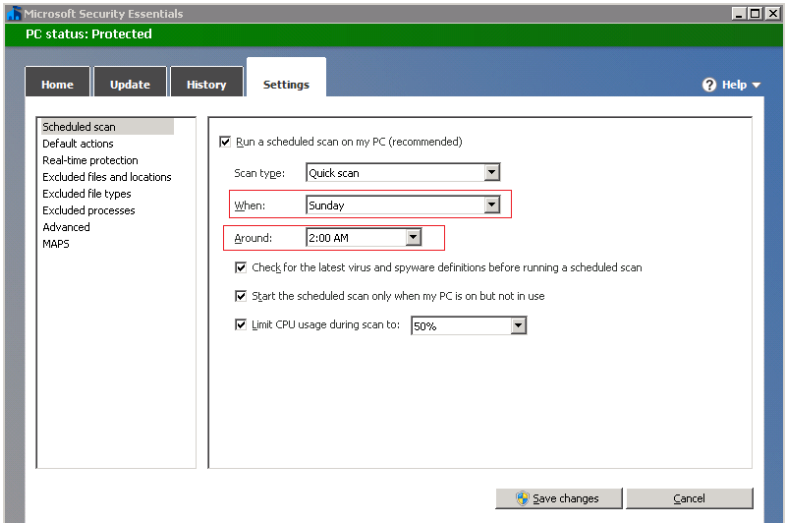
- Yêu cầu sử dụng phần mềm diệt virus luôn ở chế độ bảo vệ.



- Cập nhật các mẫu diệt virus mới hàng ngày.



- Quét toàn bộ máy chủ theo định kỳ tối thiểu 1 tháng 1 lần: Chỉ yêu cầu bắt buộc đối với các hệ thống public.



8. Yêu cầu môi trường vận hành an toàn

- User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP).

- Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho máy người dùng cuối để vận hành hệ thống .

- Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MS Office/pdf.

Phụ lục 06.
HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT ĐỐI VỚI WEB SERVER

Hướng dẫn cấu hình với Tomcat

1. Cài đặt Web Server đảm bảo an toàn.

- Web Server phải được cài đặt trên hệ điều hành an toàn, đã được thiết lập cấu hình chính sách bảo mật theo: Tiêu chuẩn ATTT hệ điều hành.

- Phiên bản Web Server không mắc lỗ hổng bảo mật, được cập nhật tất cả bản vá security: Các Web Server Tomcat phải là phiên bản không mắc lỗi ATTT và được cập nhật các bản vá security.

2. Gỡ/tắt bỏ các thành phần mặc định khi cài đặt Web Server

- Gỡ bỏ các thư mục/trang mặc định.

+ Xóa file, thư mục tại đường dẫn CATALINA_HOME/webapps (ROOT, balancer, jsp-examples, servlet-examples, tomcat-docs, webdav, manager, docs, examples)

+ Xóa file CATALINA_HOME/conf/Catalina/localhost/host-manager.xml và CATALINA_HOME/conf/Catalina/localhost/manager.xml.

- Tắt các Module/Extension không sử dụng

+ Trên file server.xml tại đường dẫn CATALINA_HOME/conf/server.xml, tìm dòng <connector … protocol=”AJP/…”> và chuyển sang dạng ghi chú.

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<!-- <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> -->
```

+ Restart lại Tomcat.

3. Thay đổi các thành phần mặc định.

- Thay đổi thông báo lỗi mặc định của Web Server.

+ Tạo các error.html ở thư mục gốc của ứng dụng với nội dung phù hợp với từng ứng dụng.

+ Mở file web.xml tại đường dẫn CATALINA_HOME/conf/web.xml, thay đổi thông báo lỗi với các mã lỗi 400, 401, 402, 403, 404, 500, 501, 502, 503, bằng cách thêm các nội dung sau vào trước thẻ đóng </web-app>

```
<error-page>
<error-code>400</error-code>
<location>/error.html</location>
</error-page>
```

```
<error-page>
<error-code>401</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>402</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>403</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>404</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>500</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>501</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>502</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>403</error-code>
<location>/error.html</location>
</error-page>
```

+ Restart lại Tomcat.

- Chỉ cho phép thực thi các phương thức GET, POST, HEAD.

+ Mở file web.xml tại đường dẫn CATALINA_HOME/conf/web.xml thêm các dòng sau ở cuối file trước thẻ đóng </web-app>

```
<security-constraint>
<web-resource-collection>
<web-resource-name>restricted methods</web-resource-name>
<url-pattern>/*</url-pattern>
<http-method>PUT</http-method>
<http-method>DELETE</http-method>
<http-method>OPTIONS</http-method>
<http-method>TRACE</http-method>
</web-resource-collection>
<auth-constraint />
</security-constraint>
```

+ Restart lại Tomcat.

+ **Chú ý:** có thể bổ sung sử dụng PUT, DELETE với trường hợp sử dụng webservice RESTful và giao thức push của Apple.

4. Cấu hình giới hạn truy cập.

- Tắt chức năng quản trị từ xa cho Web Server, giới hạn địa chỉ IP truy cập vào trang, chức năng quản trị.

+ Mở file server.xml tại đường dẫn CATALINA_HOME/conf/server.xml -> Thêm ký tự !-- và -- vào trước và sau dòng Server address ..... "**SHUTDOWN**" để vô hiệu hóa truy cập từ xa:

```
<!--Server address="127.0.0.1" port="8005" shutdown="SHUTDOWN"-->
```

+ Restart lại Tomcat.

- Không cho phép liệt kê file, thư mục.

+ Mở file web.xml tại đường dẫn CATALINA_HOME/conf/web.xml tìm section <init-param> trong section <servlet> với ” <servlet-name>default</servlet-name>” thay đổi thuộc tính listings là false

```
<init-param>
```

```
<param-name>listings</param-name>
<param-value>false</param-value>
</init-param>
```

+ Restart lại Tomcat.

+ Đối với các trường hợp cần cấu hình cho phép Domain khác truy cập nội dung (Cross-origin resource sharing – CORS), chỉ được thêm từng domain cụ thể, không được thêm nhóm domain hoặc tất cả domain.

5. Cấu hình phân quyền ứng dụng Web Server.

- Chạy tiến trình Web Server với tài khoản user được giới hạn quyền (không phải tài khoản quản trị, hoặc có quyền tương đương với tài khoản quản trị).

+ Tạo user riêng không thuộc nhóm tài khoản quản trị (root).

+ Đăng nhập và khởi chạy ứng dụng sử dụng tài khoản vừa tạo.

- Không cho phép thực thi các câu lệnh CGI, SSI: Mặc định Tomcat đã tắt CGI.

6. Sử dụng cơ chế mã hóa an toàn.

- Không sử dụng SSL version 2.0, SSL version 3.0.

+ Mở file server.xml tại đường dẫn CATALINA_HOME/conf/server.xml, tìm và gỡ bỏ nội dung: sslProtocols=”TLS”.

+ Thêm nội dung:

```
sslEnabledProtocols=”TLSv1, TLSv1.1, TLSv1.2”
```

+ Restart lại Tomcat.

- Không sử dụng các SSLCipherSuite không an toàn: EXPORT, NULL, MD5, DES, RC4.

+ Mở file server.xml tại đường dẫn CATALINA_HOME/conf/server.xml. Tìm đến phần cấu hình SSL.

+ Cấu hình trường ciphers chỉ sử dụng các cipher an toàn:

```
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_
WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_
WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_1
28_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_RC4_128_
SHA"
```

```
    <Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
               maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
               clientAuth="false"
               sslEnabledProtocols="TLSv1, TLSv1.1, TLSv1.2"
               keystoreFile="/home/test/test.jks"
               keystoreType="JKS"
               keystorePass="123456"
               keyPass="123456"
               ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_R
SA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_A
ES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA,
SSL_RSA_WITH_RC4_128_SHA"
                />
```

+ Restart lại Tomcat.

7. Cấu hình ghi log Web Server an toàn

- Web Server cần được thiết lập bật chế độ ghi log, ghi luân phiên/xoay vòng log file theo ngày

+ Mở file server.xml tại đường dẫn CATALINA_HOME/conf/server.xml.

+ Bổ sung thêm đoạn cấu hình sau vào server.xml nếu chưa có:

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
prefix="<TEN APP>_"
suffix=".log"
pattern="%h %{X-Forwarded-For}i %l %u %t &amp;quot;%r&amp;quot; %s %b &amp;quot;%{Referer}i&amp;quot; &amp;quot;%{User-Agent}i&amp;quot;"
resolveHosts="false"
fileDateFormat="yyyy-MM-dd"
rotatable="true" />
```

+ Trong đó:
  - directory: Thư mục đặt file log.
  - prefix: Tiền tố tên file.
  - suffix: Phần tên đuôi file.
  - pattern: Định nghĩa các trường ghi trong access log
  - resolveHosts: Có phân giải IP thành tên miền hay không? (true, false)
  - fileDateFormat: Là định dạng in ngày tháng, mặc định nếu không đặt thì mặc định sẽ là “yyyy-MM-dd”
  - rotatable: là biến cho phép rotate log hàng ngày, mặc định là true, tuy nhiên nếu là false thì biến fileDateFormat sẽ không có tác dụng.

+ Restart lại Tomcat.

- Định dạng dữ liệu log phải có đủ thông tin phục vụ cho việc điều tra, truy vết vi phạm ATTT: Thực hiện trong bước trên.

- Log cần được lưu trữ tối thiểu 03 tháng trên máy chủ.

+ Dựa vào dung lượng log trung bình 01 ngày, cần chuẩn bị dung lượng ổ cứng để lưu được log tối thiểu 90 ngày.

+ Đặt lịch xóa file log lâu hơn 90 ngày nếu cần thiết để tránh đầy ổ cứng.

+ Các đơn vị chủ động đẩy log định kỳ hàng ngày lên file server chung, đảm bảo lưu trữ 03 tháng, nén định dạng zip.

Phụ lục 07.
HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT ĐỐI VỚI WEB SERVER

Hướng dẫn cấu hình với Apache

1. Cài đặt Web Server đảm bảo an toàn

- Web Server phải được cài đặt trên hệ điều hành an toàn, đã được thiết lập cấu hình chính sách bảo mật: Tham chiếu mục 1 Tiêu chuẩn ATTT hệ điều hành.

- Phiên bản Web Server không mắc lỗ hổng bảo mật, được cập nhật tất cả bản vá security:

+ Đối với các hệ thống cài mới: Sử dụng Apache phiên bản mới nhất (Tham khảo tại: http://httpd.apache.org/download.cgi).

+ Các Web Server Apache phải được cập nhật các bản vá security.

- Không sử dụng các bộ cài tích hợp sẵn như: xampp, wampp, appserver.

2. Gỡ/tắt bỏ các thành phần mặc định khi cài đặt Web Server

- Gỡ bỏ các thư mục/trang mặc định như trang ví dụ, hướng dẫn, các trang quản trị web server từ xa, xác trang phục vụ dev, debug

+ Thực hiện xóa bỏ trang mặc định của apache khi cài đặt trong thư mục /var/www/html/

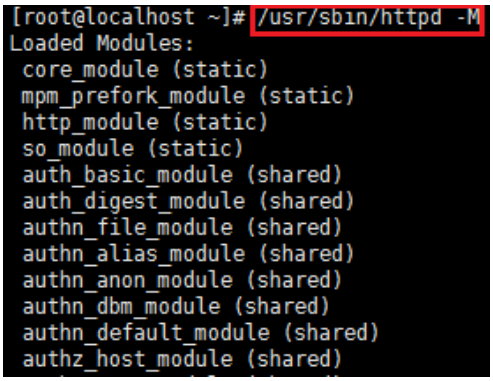
+ Xóa các trang ví dụ, hướng dẫn, các trang quản trị web server từ xa, xác trang phục vụ dev, debug,..

- Tắt các Module/Extension không sử dụng

+ Bước 1: Kiểm tra các modules được load:

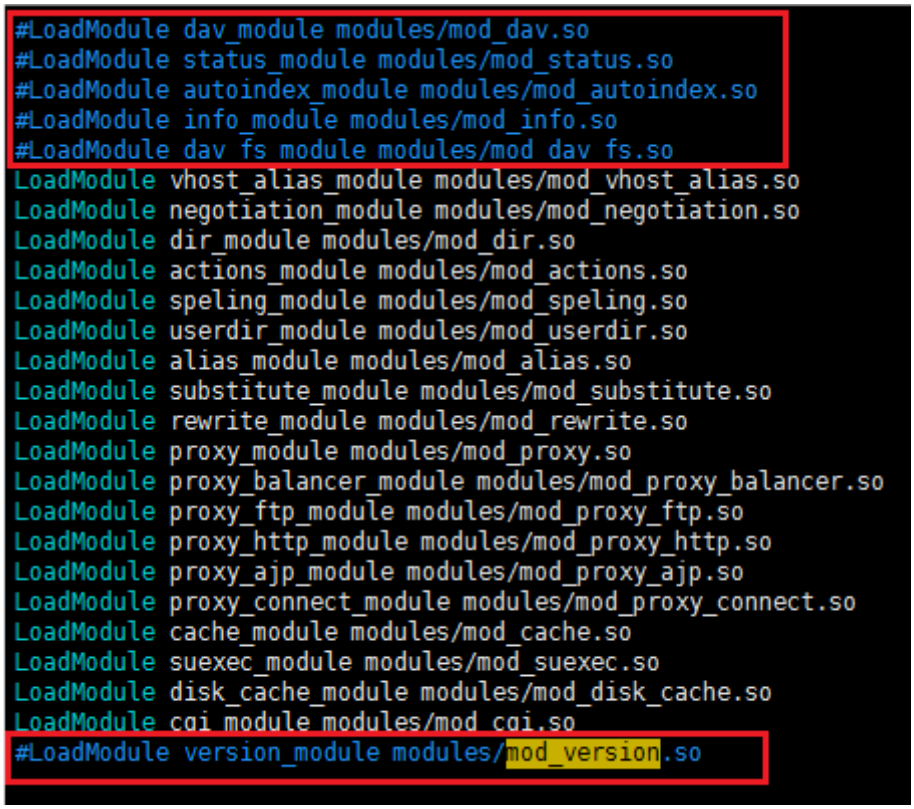
Sử dụng lệnh: # /usr/sbin/httpd -M Hoặc: # grep LoadModule /etc/httpd/conf/httpd.conf

+ Kết quả sẽ hiển thị các module được load.



```
[root@localhost ~]# grep LoadModule /etc/httpd/conf/httpd.conf
# have to place corresponding `LoadModule' lines at this location so the
# LoadModule foo_module modules/mod_foo.so
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule authn_alias_module modules/mod_authn_alias.so
LoadModule authn_anon_module modules/mod_authn_anon.so
LoadModule authn_dbm_module modules/mod_authn_dbm.so
```

+ Mở file httpd.conf thêm dấu # vào đầu dòng load modules, mà không cần sử dụng. Ví dụ một số modules có thể loại bỏ như (mod_info, mod_status, mod_version, mod_autoindex, mod_dav)



+ Restart lại Apache.

3. Thay đổi các thành phần mặc định

- Thay đổi thông báo lỗi mặc định của Web Server.

+ Tạo file error.html tại thư mục gốc của website (Thư mục mặc định là /var/www/html).

+ Thêm nội dung sau vào file httpd.conf:

```
ErrorDocument 400 /error.html
ErrorDocument 401 /error.html
ErrorDocument 402 /error.html
ErrorDocument 403 /error.html
ErrorDocument 404 /error.html
```

```
ErrorDocument 500 /error.html
ErrorDocument 501 /error.html
ErrorDocument 502 /error.html
```

+ Restart lại Apache.

- Thay đổi thông tin banner của dịch vụ HTTP, không để lộ thông tin phiên bản hệ điều hành, Web Server.

+ Mở file httpd.conf và thêm thuộc tính như sau:

```
ServerSignature Off
ServerTokens Prod
```

+ Restart lại Apache.

- Chỉ cho phép thực thi các phương thức GET, POST, HEAD:

+ Mở file httpd.conf và thêm thuộc tính LimitExcept như sau:

```
<Directory "/var/www/web">
<LimitExcept GET POST HEAD>
Deny from all
</LimitExcept>
...
</Directory>
```

+ Restart lại Apache.

+ Cho phép sử dụng PUT, DELETE với trường hợp sử dụng Webservice RESTful và giao thức PUSH của Apple.

4. Cấu hình giới hạn truy cập

- Giới hạn địa chỉ IP truy cập vào trang, chức năng quản trị: Các chức năng quản trị như: quản trị CMS, quản trị trang admin (của Sharepoint) phải tiến hành giới hạn chính xác các IP được truy cập, không cho phép truy cập trực tiếp từ bất kỳ địa chỉ IP nào ngoài Internet. Việc giới hạn có thể thực hiện bằng tính năng của ứng dụng web, hoặc bằng cấu hình tường lửa mềm trên hệ điều hành (Tham khảo trong Baseline thiết lập cấu hình an toàn hệ điều hành).

- Không cho phép liệt kê file, thư mục.

+ Thêm thuộc tính ” **-Indexes**” vào thẻ (Directory) trong file httpd.conf:

```
<Directory "/var/www/web">
 Options -Indexes
```

```
</Directory>
```

+ Lưu ý: Đường dẫn tới thư mục website "/var/www/web" tùy thuộc vào thư mục đặt website trên server.

+ Restart lại Apache.

+ Đối với các trường hợp cần cấu hình cho phép Domain khác truy cập nội dung (Cross-origin resource sharing – CORS), chỉ được thêm từng domain cụ thể, không được thêm nhóm domain hoặc tất cả domain.

5. Cấu hình phân quyền ứng dụng Web Server

- Chạy tiến trình Web Server với tài khoản user được giới hạn quyền (không phải tài khoản quản trị, hoặc có quyền tương đương với tài khoản quản trị).

+ Bước 1: Tạo tài khoản www-data để chạy Apache

```
# useradd –M www-data –s /bin/false
hoặc # useradd –d /dev/null –s /bin/false www-data
```

+ Không cho phép đăng nhập vào tài khoản chạy Apache:

```
# passwd –l www-data
```

+ Phân quyền cho thư mục web, chỉ cho phép tài khoản www-data và nhóm www-data có quyền thay đổi trong thư mục /var/www.

```
# chown -R www-data: www-data /var/www
# find /var/www -type d | xargs chmod -R 755
# find /var/www -type f  | xargs chmod -R 644
# chown -R www-data:www-data [Đường_dẫn_tuyệt_đối_cache/session]
```

+ Bước 2: Cấu hình tài khoản chạy Apache: Thay đổi tài khoản dùng để chạy Apache trong file: /etc/httpd/conf/httpd.conf

+ Tìm đến đoạn sau.

```
User root (thay đổi tới tài khoản www-data)
Group root (thay đổi tới nhóm www-data)
```

+ Restart lại Apache.

- Không cho phép thực thi các câu lệnh CGI, SSI

+ Thêm thuộc tính ” **–ExecCGI**” vào thẻ (Directory) trong file httpd.conf:

```
<Directory /var/www/web>
Options –ExecCGI -Includes
</Directory>
```

+ Lưu ý: Đường dẫn tới thư mục website “/var/www/web” tùy thuộc vào thư mục đặt website trên server.

+ Restart lại Apache.

6. Sử dụng cơ chế mã hóa an toàn

- Sử dụng thư viện mã hóa an toàn:

+ Đối với các hệ thống cài mới: Sử dụng phiên bản thư viện OpenSSL mới nhất.

+ Các hệ thống sử dụng bộ thư viện OpenSSL phải được nâng cấp, cập nhật các bản vá security đã được cảnh báo.

- Không sử dụng SSL version 2.0, SSL version 3.0.

+ Bước 1: Tìm file cấu hình SSL cho Apache: Sử dụng lệnh:

```
#grep –i –r ”SSLProtocol” /etc/httpd
```

```
[root@localhost certs]# grep -i -r "SSLPro" /etc/httpd/
/etc/httpd/conf.d/ssl.conf:SSLProtocol all -SSLv2
Binary file /etc/httpd/modules/mod_ssl.so matches
```

+ Trong đó /etc/httpd là thư mục cài đặt httpd. Kết quả trả về thu được đường dẫn file cấu hình SSL: /etc/httpd/conf.d/ssl.conf.

+ Bước 2: Mở file /etc/httpd/conf.d/ssl.conf và thay đổi: SSLProtocol all (có thể có –SSLv2) thành:

```
SSLProtocol all –SSLv2 –SSLv3
```

+ Restart lại Apache.

- Thiết lập SSLCipherSuite an toàn cho webserver.

+ Trong file cấu hình SSL của Apache, cấu hình trường SSLCipherSuite chỉ sử dụng các cipher an toàn và bỏ đi các cipher không an toàn:

```
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-
ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-
AES128-GCM-SHA256:DHE-DSS-AES128-GCM-
SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-
ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-
ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-
```

ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:**!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK:!SSLv3:!SSLv2**

+ Restart lại Apache.

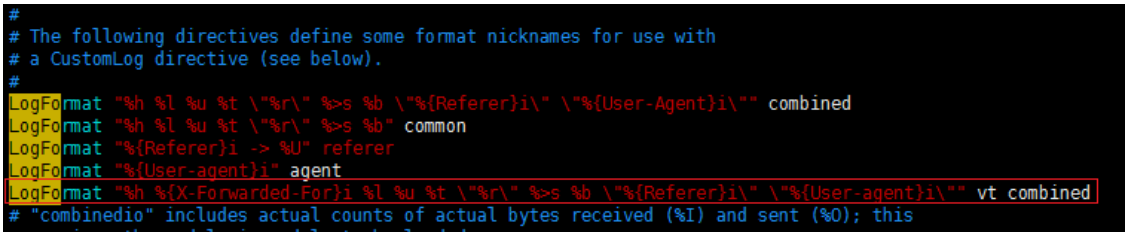
7. Cấu hình ghi log Web Server an toàn

- Đồng bộ thời gian cho máy chủ web với máy chủ thời gian, đảm bảo thời gian ghi trong log file là chính xác và đồng nhất: Tham khảo cấu hình ATTT cho hệ điều hành.

- Định dạng dữ liệu log phải có đủ thông tin phục vụ cho việc điều tra, truy vết vi phạm ATTT.

+ Mở file cấu hình httpd.conf, tìm đến đoạn định nghĩa LogFormat, bổ sung thêm một LogFormat mới tên là vt_combined cho Apache:

```
LogFormat "%h %{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\"" vt_combined
```



+ Restart lại Apache.

- Web Server cần được thiết lập bật chế độ ghi log, ghi luân phiên/xoay vòng log file theo ngày

+ Để cấu hình xoay vòng log theo ngày, ta tìm đến đoạn cấu hình log access, log error của Apache (từ khóa là CustomLog, ErrorLog), sửa thành:

```
CustomLog "|/path/to/rotatelogs /path/to/log/httpd/<Tên_APP>_%Y-%m-%d.log 86400" vt_combined

ErrorLog "|/path/to/rotatelogs /path/to/log/httpd/<Tên_APP>_error_%Y-%m-%d.log 86400"
```

+ **Lưu ý:** Mặc định khi cài apache theo dạng RPM hay APT-GET thì Linux có sẵn 1 chương trình xoay vòng log tên là "logrotate httpd". Tuy nhiên khi dùng chương trình này thì mỗi lần xoay vòng log thì phải khởi động lại apache server,

do đó ta thống nhất sử dụng "rotatelogs" của apache và xóa cấu hình của "logrotate httpd" của hệ điều hành đi.

+ Restart lại Apache.

- Log cần được lưu trữ tối thiểu 03 tháng trên máy chủ.

+ Dựa vào dung lượng log trung bình 01 ngày, cần chuẩn bị dung lượng ổ cứng để lưu được log tối thiểu 90 ngày.

+ Đặt lịch xóa file log lâu hơn 90 ngày nếu cần thiết để tránh đầy ổ cứng.

+ Các đơn vị chủ động đẩy log định kỳ hàng ngày lên file server chung, đảm bảo lưu trữ 03 tháng, nén định dạng zip.

8. Cấu hình bảo mật cho PHP

- Ngăn chặn Remote code Execute:

+ Mở file php.ini, thiết lập:

```
allow_url_fopen = Off
```

+ Restart lại Apache.

- Giới hạn thư mục Php truy cập.

+ Mở file php.ini, thiết lập

```
open_basedir = /var/www:/path/to/first/folder:/path/to/second/folder
```

+ /var/www:/path/to/first/folder

- Vô hiệu hóa các hàm thực thi tới hệ thống không cần thiết.

+ Mở file php.ini, thiết lập các hàm cần vô hiệu hóa như bên dưới:

```
disable_functions =
exec,passthru,shell_exec,system,proc_open,popen,curl_exec,
curl_multi_exec,parse_ini_file,show_source, symlink
```

+ Restart lại Apache.

- Loại bỏ các modules không cần thiết.

+ Sử dụng lệnh sau để xem các module đã được load

```
php -m
```

+ Sau đó sử dụng lệnh

```
Locate tên_module (để xác định vị trí của module)
mv /đường_dẫn_tới_module_cần_backup/newname.backup
```

+ Restart lại Apache.

9. Yêu cầu môi trường vận hành an toàn

- User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP).

- Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho máy người dùng cuối để vận hành hệ thống .

- Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MSOffice/pdf.

Phụ lục 08.
HƯỚNG DẪN THIẾT LẬP QUY TẮC CẤU HÌNH ATTT CHO HỆ QUẢN TRỊ CƠ CỞ DỮ LIỆU

I. Hướng dẫn với Oracle

1. Cài đặt Hệ quản trị CSDL an toàn.

1.1.Hệ quản trị CSDL phải được cài đặt trên hệ điều hành an toàn.

Yêu cầu: Hệ quản trị CSDL phải được cài đặt trên hệ điều hành an toàn, đã được thiết lập cấu hình chính sách bảo mật (tham chiếu Hướng dẫn thiết lập chính sách bảo mật cho hệ điều hành).

1.2. Hệ quản trị CSDL phải được cài đặt trên hệ điều hành an toàn.

Phiên bản Hệ quản trị CSDL không mắc lỗ hổng bảo mật đã được công bố, được cập nhật tất cả bản vá security (nếu có).

2. Gỡ bỏ/tắt các thành phần thừa, thành phần không sử dụng.

2.1.Xóa các tài khoản, các CSDL thừa, không sử dụng.

Xóa các tài khoản, các CSDL thừa, không sử dụng.

- Tài khoản không sử dụng là tài khoản chưa login vào database trong vòng 3 tháng gần nhất hoặc các tài khoản mặc định trên oracle không dùng đến.

Bước 1: Kiểm tra toàn bộ các tài khoản đang tồn tại trên hệ thống.

```
SELECT * FROM dba_users;
```

Bước 2: Kiểm tra xem user nào không sử dụng thì thực hiện khóa lại với câu lệnh sau:

```
ALTER USER <user_name> ACCOUNT LOCK;
```

2.2.Thay đổi tên mặc định của tài khoản quản trị.

Không áp dụng với hệ quản trị cơ sở dữ liệu Oracle.

2.3.Tắt các hàm tương tác với tài nguyên hệ điều hành (hàm đọc, ghi file, thực thi câu lệnh hệ thống).

Tắt các hàm tương tác với tài nguyên hệ điều hành (hàm đọc, ghi file, thực thi câu lệnh hệ thống).

- Thu hồi quyền "Alter system":

+ Kiểm tra tài khoản có quyền "Alter system"

```
SELECT * FROM dba_sys_privs WHERE GRANTEE IN (SELECT username FROM dba_users WHERE account_status='OPEN') AND PRIVILEGE = 'ALTER SYSTEM';
```

+ Thu hồi quyền Alter system của tài khoản không cần thiết.

```
REVOKE ALTER SYSTEM FROM username;
```

- Thu hồi quyền DBA:

+ Kiểm tra tài khoản có quyền quản trị DBA:

```
SELECT * FROM dba_role_privs WHERE granted_role='DBA' AND GRANTEE IN (SELECT DISTINCT username FROM dba_users WHERE account_status='OPEN');
```

+ Thu hồi quyền dba của tài khoản:

```
REVOKE dba FROM username
```

3. Thiết lập chính sách tài khoản.

3.1. Các ứng dụng không dùng tài khoản có quyền quản trị để kết nối đến CSDL.

Các ứng dụng không dùng tài khoản có dba, alter system để kết nối đến CSDL.

Kiểm tra tài khoản của ứng dụng không và thu hồi quyền không cần thiết như mục 2.3.

3.2. Tất cả các tài khoản phải có mật khẩu.

Các tài khoản trên cơ sở dữ liệu phải có mật khẩu.

- Đối với Oracle phiên bản từ 10 trở xuống.

+ Kiểm tra các user mật khẩu khẩu rỗng.

```
select username,password from dba_users where password is null;
```

+ Đặt mật khẩu cho các user không có mật khẩu:

```
alter user username identified by "password_khó"
```

- Đối với Oracle phiên bản từ 11 trở lên.

+ Kiểm tra các user mật khẩu rỗng.

```
select name, password from sys.user$
where name in (select username from dba_users) and PASSWORD is null
```

+ Đặt mật khẩu cho các user không có mật khẩu.

```
alter user username identified by "password_khó"
```

3.3. Các tài khoản phải được đặt mật khẩu theo đúng quy định của Tập đoàn.

Các tài khoản trên cơ sở dữ liệu phải có mật khẩu khó đảm bảo yêu cầu của Tập đoàn bao gồm: Tối thiểu 10 ký tự bao gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt chỉ áp dụng cho ***Oracle 11g.***

- Đối với user ứng dụng: Mật khẩu tối thiểu 10 ký tự bao gồm chữ, số và ký tự đặc biệt.

- Đối với user cá nhân: Thiết lập một profile riêng cho các user cá nhân, profile này yêu cầu bắt buộc đặt mật khẩu mạnh bằng cách sử dụng function có sẵn của Oracle.

Bước 1: Tạo Profile cho người dùng để đảm bảo các thuộc tính trên. Đăng nhập cơ sở dữ liệu với quyền sys để tạo profile (Ví dụ đặt tên profile là NEW_USER_PROFILE) như sau:

```
CREATE PROFILE  NEW_USER_PROFILE  LIMIT
CONNECT_TIME            3
IDLE_TIME               3
SESSIONS_PER_USER       3
CPU_PER_CALL            UNLIMITED
FAILED_LOGIN_ATTEMPTS   10
PASSWORD_LIFE_TIME      30
PASSWORD_REUSE_MAX      1
PASSWORD_LOCK_TIME      60
PASSWORD_GRACE_TIME     30
PASSWORD_VERIFY_FUNCTION VERIFY_FUNCTION_11G;
```

Bước 2: Gán user vào profile mới tạo

```
ALTER USER username
   PROFILE NEW_USER_PROFILE;
```

4. Phân quyền an toàn.

4.1. Không dùng các tài khoản quản trị, nhóm quản trị: root, Administrator, Local System,... để chạy dịch vụ CSDL.

- Với CSDL mới cần tạo tài khoản hệ điều hành riêng để chạy dịch vụ CSDL.

- Với CSDL đang chạy kiểm tra tài khoản chạy dịch vụ CSDL thuộc nhóm, nếu thuộc nhóm root, administrator hoặc Local System cần thực hiện tạo tài khoản hoặc thu hồi quyền thuộc nhóm root, administrator của tài khoản chạy dịch vụ CSDL.

- Đối với Linux:

Trường hợp 1: Với các cơ sở dữ liệu Oracle cài mới. Thực hiện các bước sau:

```
#groupadd oinstall
#groupadd dba
#groupadd oper
#groupadd asmadmin

#useradd -g oinstall -G dba,oper,asmadmin oracle
passwd <Nhập password mạnh ở đây>

#mkdir -p /u01/app/oracle/product/11.2.0/db_1
#chown -R oracle:oinstall /u01
#chmod -R 775 /u01
# su – oracle
$ cd /u01/[Oracle Source]
$ ./runInstaller
```

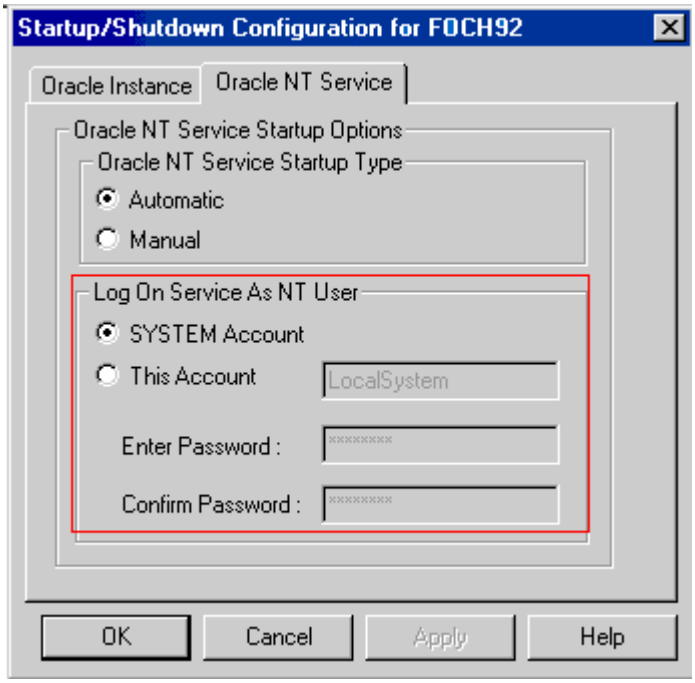
Trường hợp 2: Với các cơ sở dữ liệu Oracle đã cài đặt. Thực hiện các bước sau:

```
usermod -g <normal_group> oracle……
```

- Đối với Windows:

+ Sử dụng tiện ích: Administration Assistant for Windows NT của Oracle

+ Click chuột phải vào sid của instance đang chạy chọn ”Startup/Shutdown Options”. Chọn tab ”Oracle NT Service”.



+ Trong tab ”Oracle NT Service” chỉnh sửa account chạy oracle trong phần ”Log On Service As NT User”

4.2. Phân quyền chỉ cho phép tài khoản chạy dịch vụ CSDL được phép truy cập đến các thư mục chứa file dữ liệu, file log của CSDL.

- Kiểm tra, thay đổi đảm bảo chỉ có user oracle và group osdba có quyền trên thư mục oracle_home.

- Kiểm tra chủ sở hữu và nhóm chủ sở hữu của toàn bộ các file trong thư mục gốc Oracle, đảm bảo chủ sở hữu là tài khoản quản trị hệ cơ sở dữ liệu và nhóm sở hữu là nhóm của osdba đối với database chạy single. Riêng đối với database chạy RAC, nhóm quyền sẽ đặc biệt hơn, một số file sẽ thuộc nhóm osdba, một số file user root sẽ quản lý.

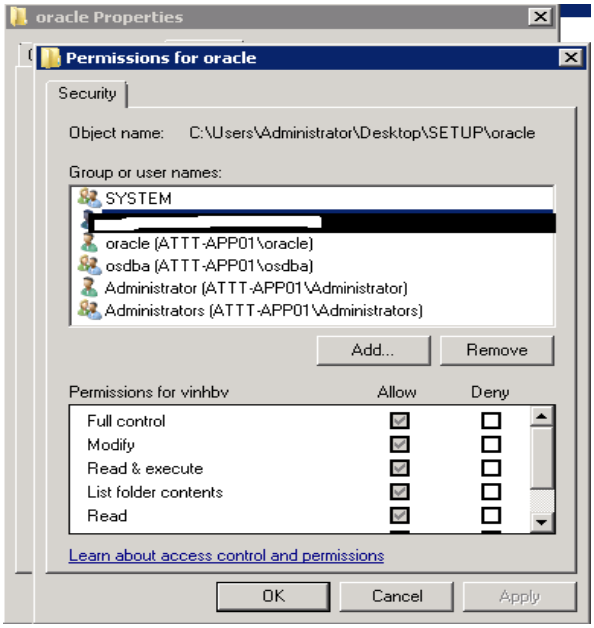
+ Với Linux/Unix:

```
#chown oracle:osdba <oracle_home_dir>
```

+ Với Windows:

Bước 1: Click chuột phải vào thư mục home gốc của oracle/ Chọn thẻ Security.

Bước 2: Trong cửa sổ ”Permissions for...” hiện ra, đảm bảo chỉ có user oracle, administrator và nhóm osdba, Administrator, System có quyền trên thư mục này như hình bên dưới:



4.3. Với mỗi ứng dụng, tạo một tài khoản kết nối CSDL riêng và chỉ cấp quyền tối thiểu đảm bảo hoạt động của ứng dụng.

- Rà soát đảm bảo user ứng dụng đảm bảo các yêu cầu sau:

+ User ứng dụng phải đặt riêng trên một tablespace mặc định, không trùng với tablespace SYSTEM, SYSAUX hoặc các tablespace mặc định của Oracle.

+ User ứng dụng tạo ra chỉ có các quyền cơ bản, cần thiết cho ứng dụng chạy như: connect, resource, create view, create sequence.

+ Đối với các ứng dụng cần quyền trên một user ứng dụng khác, thì quyền được cấp phải chính xác đến đối tượng (table, view, sequence..) mà ứng dụng cần, không được cấp quyền any hoặc quyền không chính xác.

CREATE USER APP identified by "PASSWORD" default tablespace DATA;

GRANT CONNECT, RESOURCE, CREATE VIEW, CREATE SEQUENCE to APP;

GRANT SELECT on CM_PRE2.SUB_MB to APP;

GRANT UPDATE on PRODUCT.PRODUCT to APP;

Cấu hình ghi log cho hệ quản trị CSDL.

Không áp dụng với CSDL Oracle.

Cấu hình giới hạn truy cập.

Giới hạn chỉ được những IP cần thiết được kết nối đến CSDL. Tham chiếu "Hướng dẫn thiết lập chính sách bảo mật cho hệ điều hành".

II. Hướng dẫn với MySQL

1. Cài đặt Hệ quản trị CSDL an toàn.

- Hệ quản trị CSDL MySQL phải được cài đặt trên hệ điều hành an toàn, ATTT hệ điều hành.

- Phiên bản MySQL không mắc lỗ hổng bảo mật, được cập nhật tất cả bản vá security:

+ Đối với hệ thống cài mới: Sử dụng MySQL phiên bản mới nhất (Tham khảo: http://dev.mysql.com/downloads/mysql).

+ Các hệ thống đang hoạt động phải được cập nhật các bản vá security.

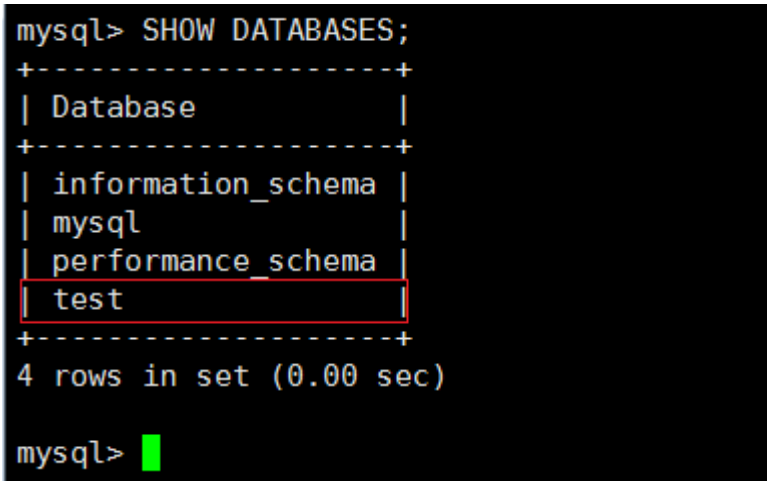
- Không sử dụng các bộ cài tích hợp sẵn như: xampp, wampp, appserver.

Gỡ bỏ/tắt các thành phần thừa, thành phần không sử dụng

Xóa các tài khoản, các CSDL thừa, không sử dụng

- Liệt kê danh sách các CSDL:

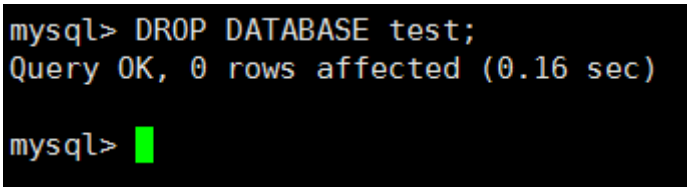
```
mysql> SHOW DATABASES;
```



Hình 1: Không được xóa các CSDL của hệ thống: information_schema, mysql, performance_schema.

- Xóa các CSDL thừa:

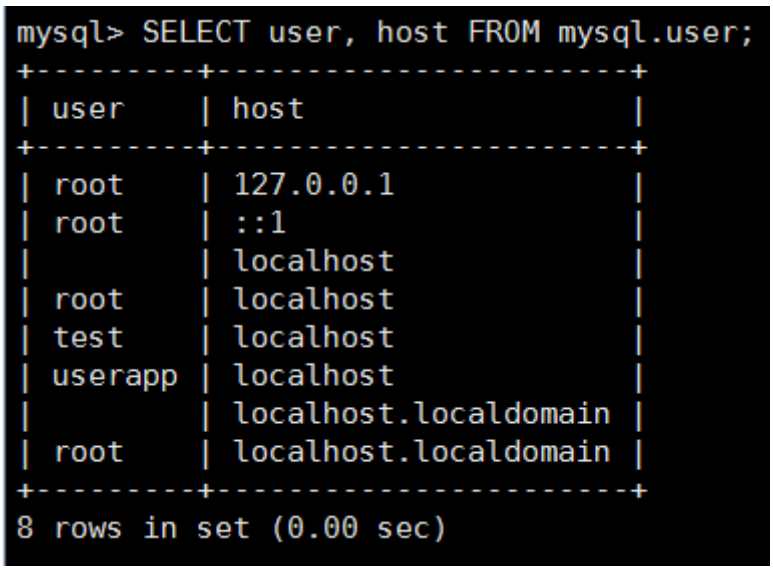
```
mysql> DROP DATABASE 'ten_CSDL';
```



Hình 2: Xóa CSDL 'test'

- Liệt kê danh sách các tài khoản có trong bảng mysql:

```
mysql> SELECT user, host FROM mysql.user;
```



Hình 3: Danh sách tài khoản.

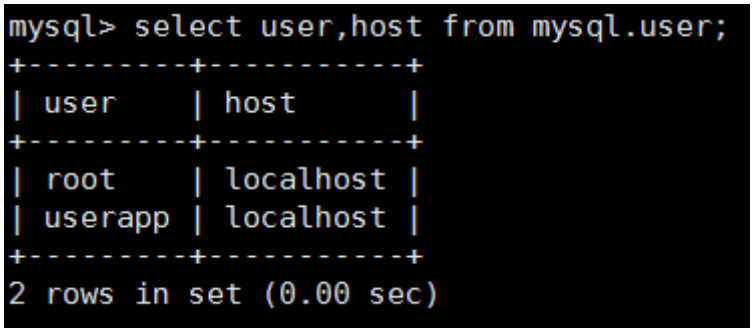
- Xóa tài khoản thừa:

Đối với phiên bản từ 5.0 trở lên có thể sử dụng:

```
mysql> DROP USER ‘ten_user’@’ten_host’;
```

Với phiên bản cũ hơn

```
mysql> DELETE FROM mysql.user WHERE user = 'ten_user' and host = 'dia_chi_host';

mysql> FLUSH PRIVILEGES;
```



Hình 4: Sau khi xóa tài khoản thừa.

Thay đổi tên mặc định của tài khoản quản trị.

- Mặc định tài khoản quản trị là ’root’, để thay đổi sử dụng câu lệnh:

Đối với phiên bản từ 5.0.2 trở lên:

```
mysql> RENAME USER root TO ten_moi;
```

Đối với phiên bản cũ hơn:

```
mysql> UPDATE user SET user = 'ten_moi' WHERE user = 'root';

mysql> FLUSH PRIVILEGES;
```

2. Tắt các hàm tương tác với tài nguyên của hệ điều hành

- Vô hiệu hóa, thu hồi các quyền tương tác với file của hệ điều hành (Xem mục 4.3)

3. Thiết lập chính sách tài khoản

Không dùng tài khoản quản trị cho các ứng dụng để kết nối đến CSDL.

- Không dùng tài khoản quản trị **root** (tài khoản đã đổi tên có quyền tương đương tài khoản **root**) cho các ứng dụng kết nối tới CSDL.

Tất cả các tài khoản phải có mật khẩu

- Liệt kê danh sách các tài khoản không có mật khẩu

```
mysql> SELECT user,host,password FROM mysql.user WHERE password = '';
```

```
mysql> SELECT user,host,password FROM mysql.user WHERE password = '';
+---------+-----------+----------+
| user    | host      | password |
+---------+-----------+----------+
| userapp | localhost |          |
+---------+-----------+----------+
1 row in set (0.00 sec)
```

Hình 5: Liệt kê tài khoản có mật khẩu rỗng.

- Đặt mật khẩu cho những tài khoản liệt kê được, mật khẩu phải tuân theo đúng quy định của Tập đoàn (tham khảo mục 3.3).

Các tài khoản phải được đặt mật khẩu theo đúng quy định của Tập đoàn:

- Các tài khoản phải có mật khẩu, mật khẩu tối thiểu 10 ký tự bao gồm: ký tự chữ, số và ký tự đặc biệt.

- Đối với tạo mới tài khoản:

```
mysql> CREATE USER 'ten_user'@'dia_chi_host' IDENTIFIED BY 'mat_khau';
```

- Đặt mật khẩu cho những tài khoản đã tồn tại:

Đối với phiên bản từ 5.0 trở lên

```
mysql> SET PASSWORD FOR 'ten_user'@'dia_chi_host' = PASSWORD('mat_khau');
```

Với phiên bản cũ hơn:

```
mysql> UPDATE mysql.user SET password  = PASSWORD('mat_khau') WHERE user = 'ten_user'
AND host ='dia_chi_host';

mysql> FLUSH PRIVILEGES;
```

4. Phân quyền an toàn

Không dùng các tài khoản quản trị, nhóm quản trị: root, Administrator, Local System,... để chạy dịch vụ CSDL.

- Kiểm tra tài khoản đang chạy dịch vụ MySQL:

```
# ps aux | grep /usr/sbin/mysqld
```

```
[root@localhost ~]# ps aux | grep /usr/sbin/mysqld
mysql     3217  0.7 86.7 1142164 422448 pts/0  Sl   14:18   0:00 /usr/sbin/mysqld --basedir=/usr
ugin-dir=/usr/lib64/mysql/plugin --user=mysql --log-error=/var/log/mysqld.log --pid-file=/var/run/
ar/lib/mysql/mysql.sock
root      3263  0.0  0.1 103244   872 pts/0    S+   14:19   0:00 grep /usr/sbin/mysqld
[root@localhost ~]#
```

Hình 6: Thông tin tiến trình chạy dịch vụ MySQL

- Kiểm tra tài khoản có thuộc nhóm quản trị không:

```
# id 'ten_tai_khoan'
```

```
[root@localhost ~]# id mysql
uid=27(mysql) gid=27(mysql) groups=27(mysql)
[root@localhost ~]#
```

Hình 7: Thông tin tài khoản chạy dịch vụ MySQL

- Kiểm tra tài khoản có được đăng nhập hay không:

```
# passwd -S 'ten_tai_khoan'
```

```
[root@localhost ~]# passwd  -S mysql
mysql LK 2015-07-10 0 99999 7 -1 (Password locked.)
[root@localhost ~]#
```

Hình 8: Đảm bảo rằng tài khoản đã bị khóa, không được đăng nhập

Phân quyền tối thiểu cho các thư mục chứa dữ liệu, thư mục chứa log, thư mục backup (nếu có)

- Thư mục chứa dữ liệu sẽ được cấu hình bởi tham số **datadir** trong file cấu hình của MySQL (/etc/my.conf). Nếu không có cấu hình này thì mặc định sẽ là /var/lib/mysql/.

- Sử dụng câu lệnh: ls –la duong_dan_thu_muc. Đảm bảo rằng các file, thư mục trong này có owner là root hoặc mysql (tài khoản chạy dịch vụ), nhóm other không được có quyền tác động.

```
[root@localhost ~]# ls -la /var/lib/mysql/
total 20500
drwxr-xr-x.  5 mysql mysql     4096 Jul 14 15:28 .
drwxr-xr-x. 17 root  root      4096 Jul 14 15:27 ..
-rw-rw----.  1 mysql mysql 10485760 Jul 14 15:28 ibdata1
-rw-rw----.  1 mysql mysql  5242880 Jul 14 15:28 ib_logfile0
-rw-rw----.  1 mysql mysql  5242880 Jul 14 15:28 ib_logfile1
drwx------.  2 mysql mysql     4096 Jul 14 15:28 mysql
srwxrwxrwx.  1 mysql mysql        0 Jul 14 15:28 mysql.sock
drwx------.  2 mysql mysql     4096 Jul 14 15:28 test
drwx------.  2 mysql mysql     4096 Jul 14 15:28 testdb
[root@localhost ~]#
```

- Kiểm tra quyền của file log: Mặc định MySQL ghi error log được cấu hình trong file my.conf với cấu hình **log-error**, kiểm tra quyền của file này:

```
[root@localhost ~]# ls -la /var/log/mysqld.log
-rw-r-----. 1 mysql mysql 1279 Jul 14 15:28 /var/log/mysqld.log
[root@localhost ~]#
```

Với mỗi CSDL của ứng dụng, tạo tài khoản riêng và chỉ cấp quyền tác động trên CSDL đó.

- Kiểm tra quyền của tài khoản

```
mysql> SHOW GRANTS FOR 'ten_tai_khoan'@'dia_chi_host';
```

```
mysql> show grants for 'userapp'@'localhost';
+-----------------------------------------------------------------------------------------------------------------+
| Grants for userapp@localhost                                                                                    |
+-----------------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'userapp'@'localhost' IDENTIFIED BY PASSWORD '*033325B717C9347C9FD49BA1F76B0D3D6253ACD9' |
| GRANT SELECT, INSERT, UPDATE, DELETE, CREATE ON `webapp`.* TO 'userapp'@'localhost'                             |
+-----------------------------------------------------------------------------------------------------------------+
2 rows in set (0.00 sec)
```

Hình 9: Xem thông tin quyền của tài khoản.

- Đảm bảo quyền global (***.***) không có các quyền **FILE**, và các quyền quản trị như **GRANT**, **SUPPER**, **PROCESS**, **RELOAD**, **SHUTDOWN**,... và chỉ có quyền tác động trên một CSDL.

- Để loại bỏ quyền của 1 tài khoản:

```
mysql> REVOKE ten_quyen ON 'ten_csdl' FROM 'ten_tai_khoan'@'dia_chi_host';

mysql> FLUSH PRIVILEGES;
```

5. Cấu hình ghi log cho hệ quản trị CSDL

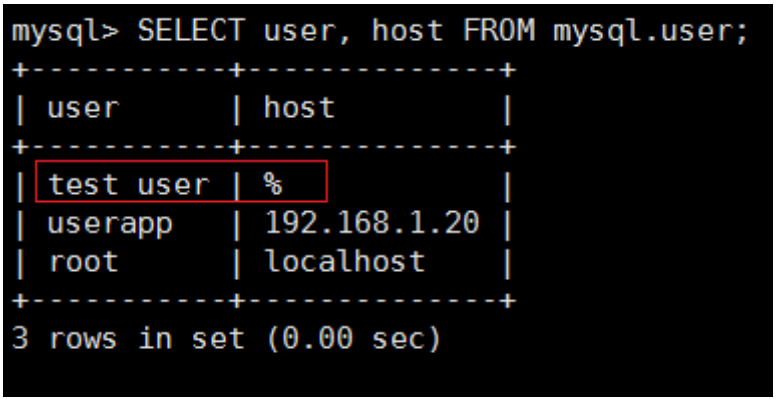
- Mặc định MySQL không có tính năng ghi auditlog.

6. Cấu hình giới hạn truy cập

Các tài khoản chỉ được kết nối từ một host cố định

- Liệt kê danh sách tài khoản

```
mysql> SELECT user, host FROM mysql.user;
```



Hình 10: Loại bỏ các tài khoản có host là '%'

Cấu hình giới hạn truy cập trên tường lửa mềm

- Cấu hình giới hạn chỉ những ip của những tài khoản liệt kê ở mục trên được kết nối tới cổng của dịch vụ.

7. Yêu cầu môi trường vận hành an toàn

- User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP).

- Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho máy người dùng cuối để vận hành hệ thống .

- Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MS Office/pdf.

Phụ lục 09.
HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HỆ THỐNG EMAIL SỬ DỤNG EXCHANGE 2016 VÀ MAIL GATEWAY FORTIMAIL

1. Yêu cầu về việc cài đặt Hệ thống email server an toàn

- Máy chủ cài đặt hệ thống email phải tuân theo tiêu chuẩn ATTT cho hệ điều hành máy chủ

- Kiểm tra các bản hotfix sử dụng lệnh

```
Get-HotFix


Source      Description      HotFixID      InstalledBy          InstalledOn
------      -----------      --------      -----------          -----------
Server01    Update           KB4495590     NT AUTHORITY\SYSTEM  5/16/2019 00:00:00
Server01    Security Update  KB4470788     NT AUTHORITY\SYSTEM  1/22/2019 00:00:00
Server01    Update           KB4480056     NT AUTHORITY\SYSTEM  1/24/2019 00:00:00
```

2. Yêu cầu môi trường vận hành an toàn

- User remote quản trị hệ thống email phải enable cơ chế xác thực đa nhân tố (token/OTP): Các user sử dụng để remote vào quản trị hệ thống mail server phải cài đặt/enable xác thực đa nhân tố. Chấp nhận sử dụng các hệ thống PIM/PAM tuy nhiên hệ thống này phải enable xác thực data nhân tố (OTP/Token)

- Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho máy người dùng cuối để vận hành các hệ thống quan trọng như AD, Proxy, Email.... Chấp nhận VDI (Virtual Desktop Infrastructure).

- Các máy riêng không dùng để sử dụng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MS Office/pdf) chỉ sử dụng để vận hành hệ thống.

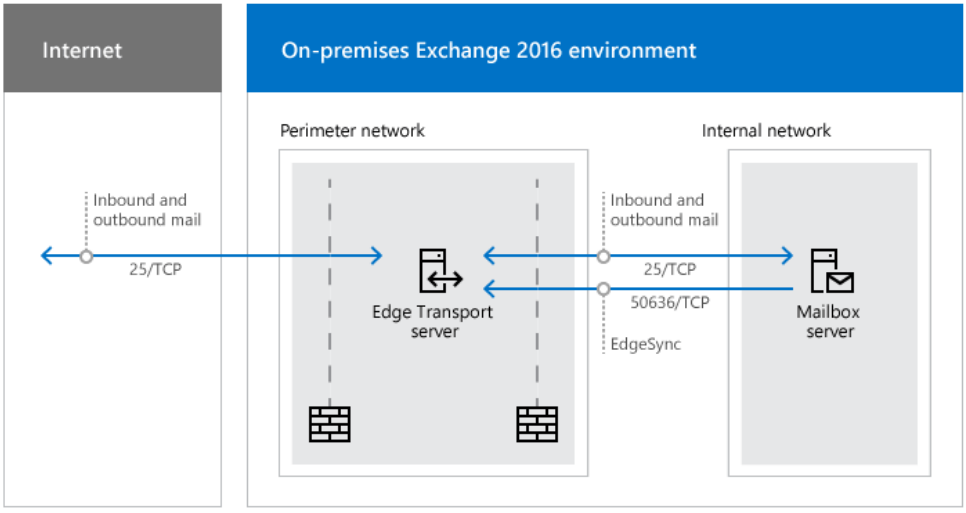
3. Yêu cầu phân tách các thành phần trong hệ thống email

- Phải có firewall quản lý chính sách traffic giữa internet và các thành phần nhận/gửi email

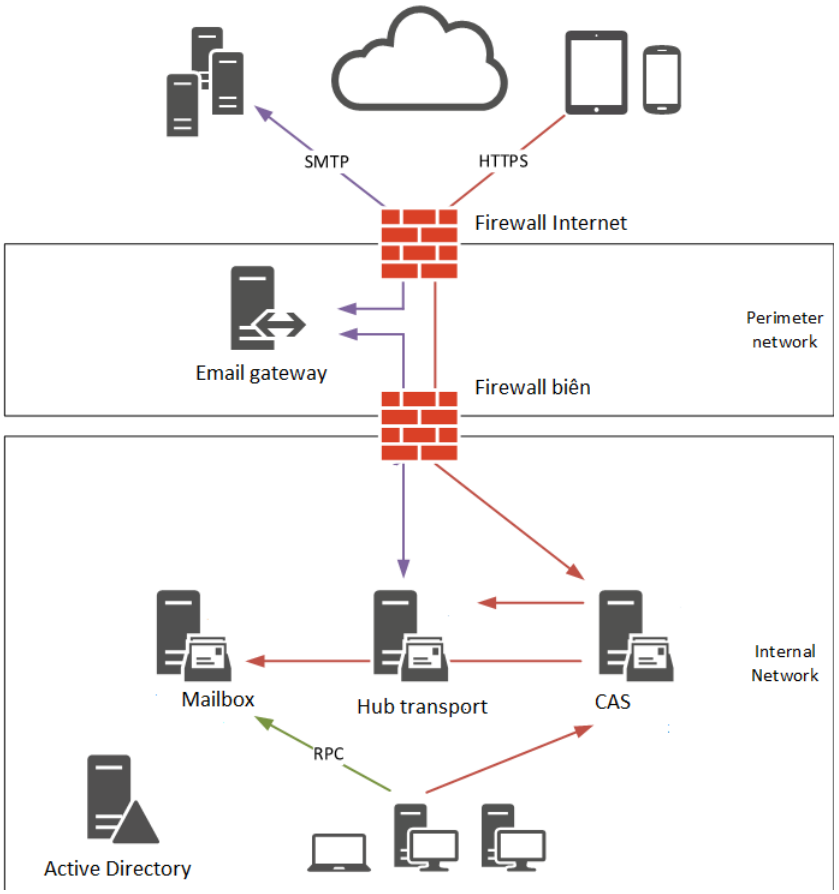
- Trường hợp có sử dụng Edge role của exchange phải phân tách thành phần này với các thành phần còn lại bằng firewall quản lý chính sách

- Topo chung có thể tham khảo khuyến cáo của microsoft

+ Trường hợp sử dụng Edge Transport



+ Trường hợp không sử dụng edge transport



4. Yêu cầu về tính sẵn sàng

- Các Role email phải có tính dự phòng. Mỗi role phải được cài đặt ít nhất trên 2 server riêng biệt ở mức vật lý.

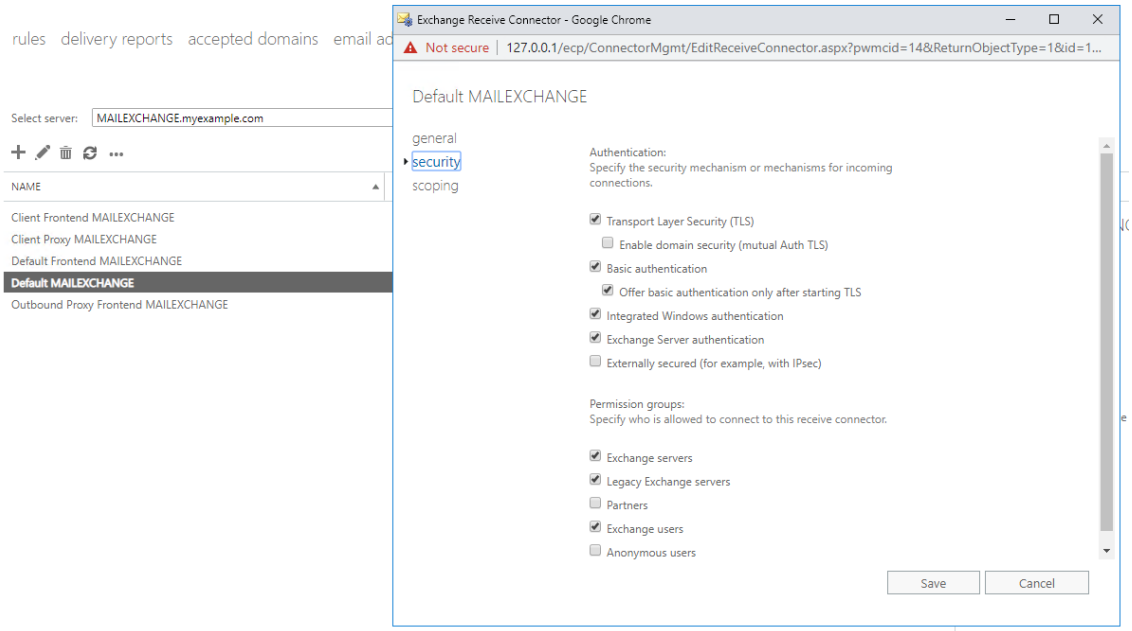
- Role Mailbox tham khảo mô hình Database Availability Group (DAG) để đảm bảo khả năng HA cho hệ thống.

- Hệ thống mailbox phải được backup định kỳ: Tham khảo các giải pháp backup enterprise của Sematic, Veeam backup,.. đảm bảo khả năng khôi phục trong trường hợp xảy ra thảm họa.

5. Yêu cầu mã hóa dữ liệu email

- Hướng dẫn enable TLS trên exchange connector

Vào EAD của server mail exchange. Mail flow -> Receive Connector. Đối với mỗi connector muốn bật sử dụng TLS trong phần security -> Tích chọn Transport Layer Security -> Save để lưu lại



6. Yêu cầu về chống email giả mạo (phishing email)

- Hướng dẫn cấu hình bản ghi SPF

+ Cách kiểm tra bản ghi 1 tên miền có bản ghi SPF hay không

Sử dụng lệnh nslookup trên Windows hoặc Linux

```
# nslookup
```

Sau đó chỉ ra 1 DNS server, có thể dùng DNS server quốc tế để kiểm tra

```
# server 8.8.8.8
```

Chỉ ra loại bản ghi SPF

```
# set type=txt
```

Chỉ ra tên miền cần kiểm tra (Chú ý nên để dấu . ở cuối cùng tên miền để truy vấn chính xác do nếu truy vấn từ các máy đang join domain thì tên miền thường hay thêm hậu tố tên domain sau cùng)

```
# abc.com.vn.
```

Nếu trả kết quả trả về có đoạn "v=spf1 ...." thì tức là tên miền có bản ghi SPF

+ Cách đọc nội dung 1 bản ghi SPF

Một bản ghi SPF bao gồm 1 danh sách, chỉ ra những máy chủ nào được phép, không được phép gửi email.

Mỗi thành phần trong danh sách bao gồm 2 phần nhỏ:

- Phần action: Mặc định không chỉ ra thì sẽ là +
  - "+": Cho phép
  - "-": Không cho phép, hard fail
  - "~": Không cho phép, soft fail
- Phần danh sách máy chủ, có nhiều cách định nghĩa máy chủ:
  - "ipv4: a.b.c.d": Chỉ ra máy chủ có IP là a.b.c.d
  - "a": Chỉ ra máy chủ trùng với bản ghi a gốc của tên miền, ví dụ bản ghi a của tên miền abc.com.vn
  - "a:domain": Chỉ ra 1 bản ghi a cụ thể, ví dụ "a:mail-in.abc.com.vn"
  - "mx": Chỉ ra máy chủ trùng với bản ghi mx của tên miền.
  - "all": Tất cả IP

Ví dụ cách đọc 1 số cách cấu hình bản ghi SPF phổ biến:

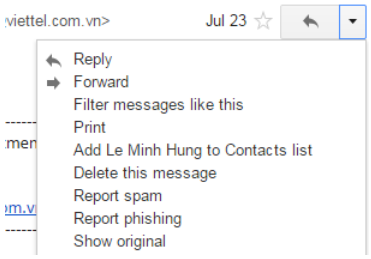
- "v=spf1 a:mail.example.com -all":
  - Cho phép máy chủ mail.example.com
  - Cấm tất cả còn lại, hard fail.
- "v=spf1 ip4:192.168.0.2 ~all":
  - Cho phép có máy chủ có IP là 192.168.0.2
  - Cấm tất cả còn lại, soft fail.
- "v=spf1 ip4:192.168.0.2 a:mail.example.com -all":
  - Cho phép có máy chủ có IP là 192.168.0.2
  - Cho phép máy chủ mail.example.com
  - Cấm tất cả còn lại, hard fail.
- "v=spf1 ip4:192.168.0.2":
  - Cho phép có máy chủ có IP là 192.168.0.2
  - Các IP còn lại thì là trung lập (neutral), không pass, không fail.

+ Cách kiểm tra bản ghi SPF của tên miền khi gửi email ra ngoài

Sau khi đã cấu hình chính xác bản ghi SPF của 1 tên miền: gửi thử nghiệm email ra 1 số email public như gmail, yahoo mail.

Đăng nhập vào gmail, yahoo mail.

Mở email vừa gửi - vào phần Show - Original



Kiểm tra trường Received-SPF: Nếu kết quả pass tức là cấu hình SPF cho phép IP được phép gửi email thành công.

Sau đó sửa bản ghi SPF, thay đổi IP hoặc tên miền sao cho IP của thành phần MTA-out không nằm trong danh sách. Đợi 30 phút để tên miền lan truyền trên internet. Sau đó gửi lại email đến gmail, yahoo mail.

Khi đấy trường Received-SPF sẽ trả về kết quả hard fail là chính xác. Nếu kết quả hard fail thì email sẽ bị đưa vào mục SPAM trong gmail, yahoo mail.

+ Cấu hình bản ghi SPF trên DNS server Bind

Thêm 1 bản ghi SPF cho tên miền với cú pháp như sau:

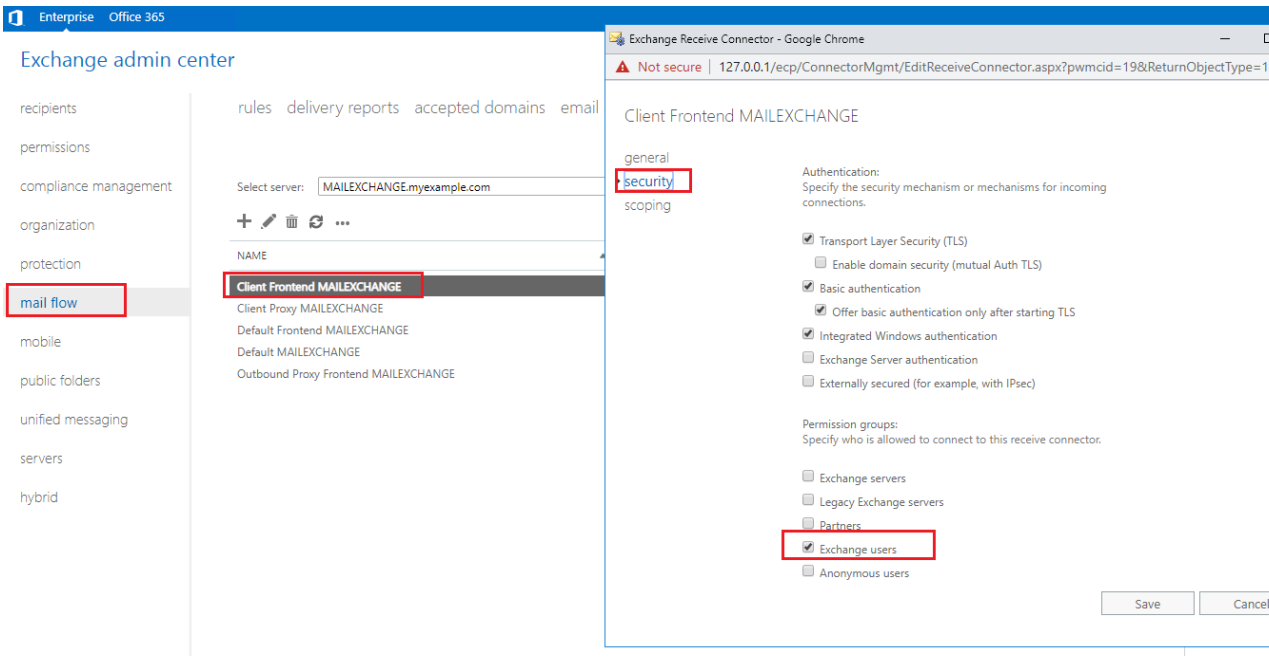
```
@           IN TXT "v=spf1 ip4:1.1.1.1 ip4:2.2.2.2 a:mta-out-01.abc.com.vn a:mta-out-02.abc.com.vn -all "
```

Trong đó:

- "@": Tên domain hiện tại
- "IN TXT": Loại bản ghi SPF là TXT
- ""v=spf1 ...."": Nội dung chính bản ghi SPF
- "ip4:1.1.1.1 ip4:2.2.2.2": Danh sách IP của thành phần MTA-out
- "a:mta-out-01.abc.com.vn a:mta-out-02.abc.com.vn": Danh sách tên của thành phần MTA-out.
- "-all": Tất cả IP còn lại đều không được phép gửi mail, hard fail.

- Hướng dẫn yêu cầu xác thực trước khi gửi mail trong luồng email nội bộ

+ Vào EAD của server mail exchange. Mail flow -> Receive Connector. Đối với mỗi connector nhận email cần auth vào phần Security -> Tích chọn Exchange Users -> Save để lưu lại



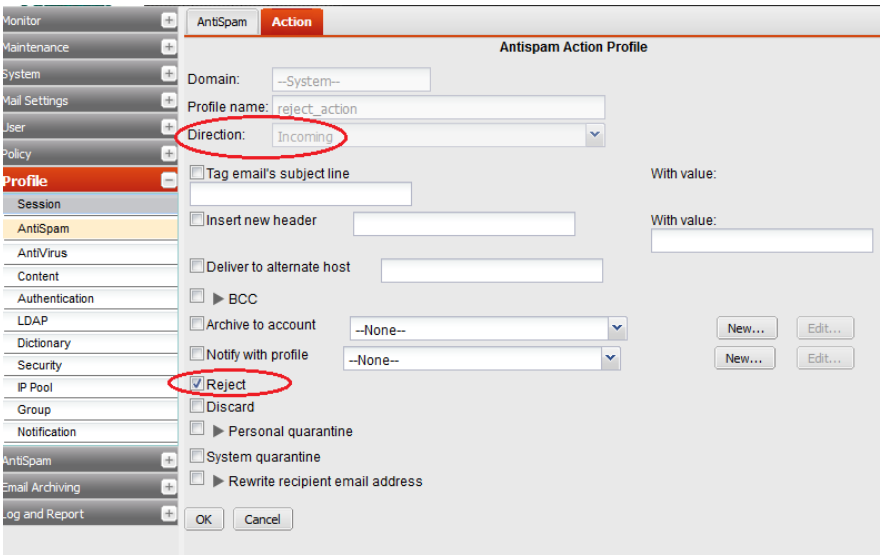
Chú ý: Tuyệt đối không tích chọn Anonymous users trừ khi là Connector nhận mail từ mail gateway

- Hướng *dẫn cấu hình check SPF khi nhận được email từ email server bên ngoài*

+ Đối với thành phần MTA-in là Fortimail

Vào Profile - Antispam - chọn Tab Action

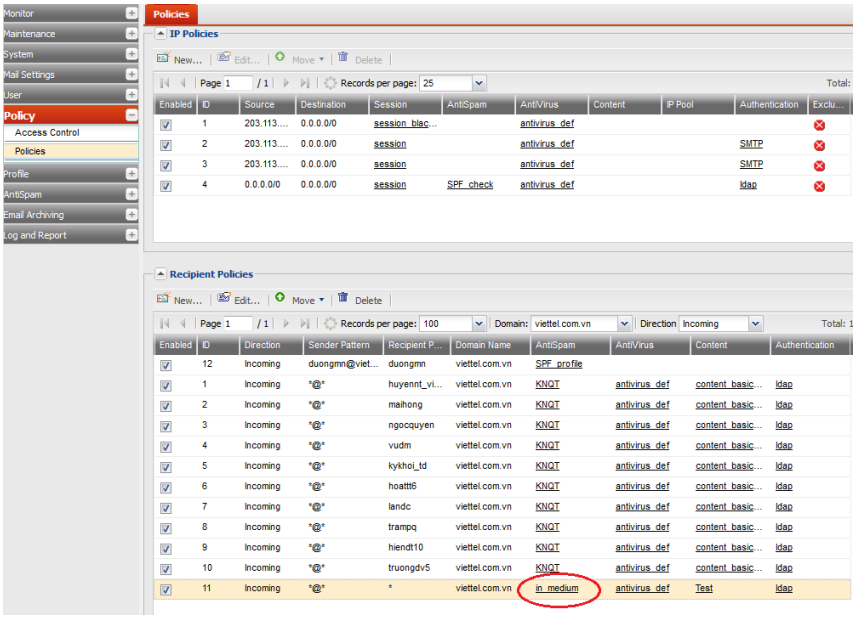
Nếu chưa có action là có Direction là Incoming và Action là Reject thì cần tạo mới 1 action như vậy, lưu ý Direction là Incoming và Action là Reject



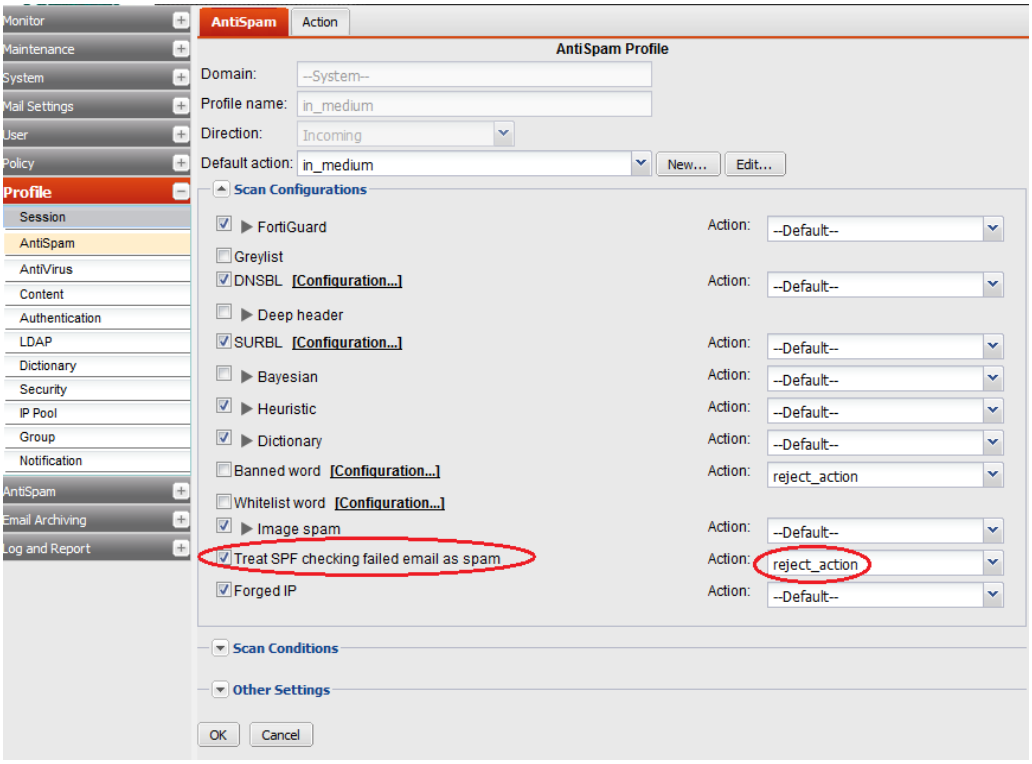
Sửa Antispam profile đang sử dụng hoặc nếu chưa sử dụng Antispam profile nào thì cần tạo mới (Trong Profile - AntiSpam) và áp dụng.

- Cách kiểm tra Antispam profile đang sử dụng thì vào phần Policy - Policies - Recipient Policies. Tìm kiếm theo Direction là Incomming, domain cần cấu hình profile, Receipient Pattern là *,

khi đó trong mục Antispam profile sẽ hiển thị profile hiện tại đang được áp dụng hiện tại.



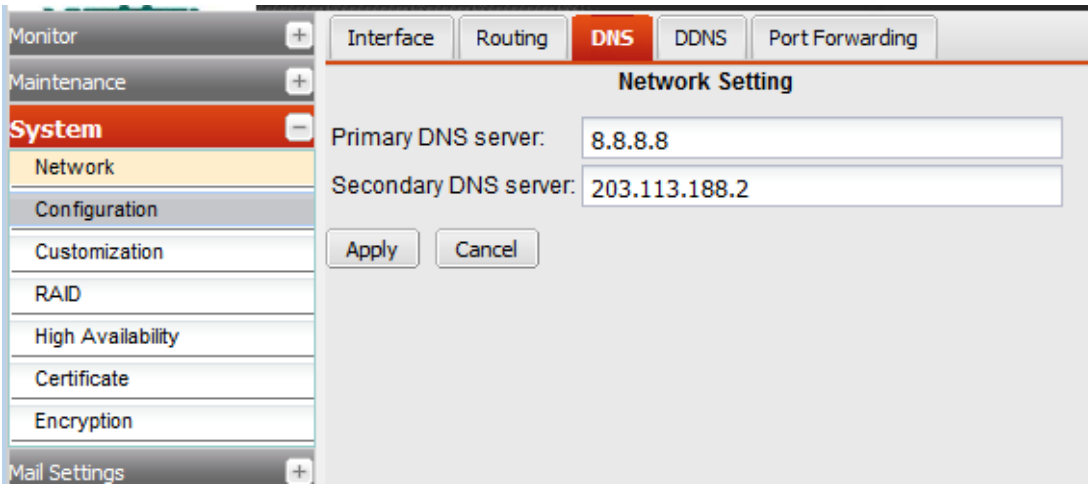
Trong Antispam profile cần sửa tích chọn Treat SPF checking failed email as spam và Action là reject action đã tạo ở trên.



Mặc định Fortimail chỉ coi nếu kiểm tra SPF trả về hard fail thì mới coi là spam, còn soft fail thì chưa coi là spam, do đó cần cấu hình Fortimail để coi soft fail cũng là spam bằng cách gõ lệnh sau trên CGI:

```
config antispam settings
        set spf-checking aggressive
```

Chú ý để kiểm tra được bản ghi SPF cho Fortimail thì cần cấu hình chính xác thông tin về DNS server cho Fortimail, nếu cấu hình sai DNS hoặc Fortimail không truy vấn được bản ghi DNS thì sẽ không kiểm tra được SPF. Để kiểm tra cấu hình DNS vào phần System - Network - DNS

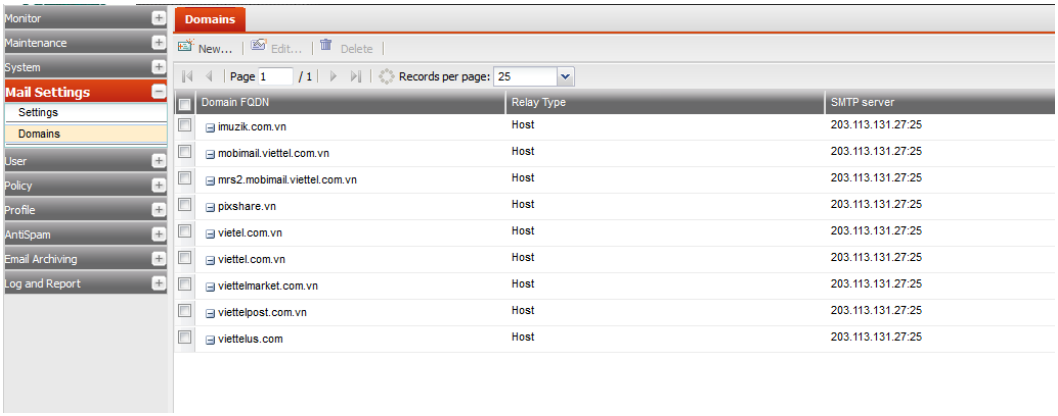


7. Yêu cầu về chống email spam

- Không cho phép open relay

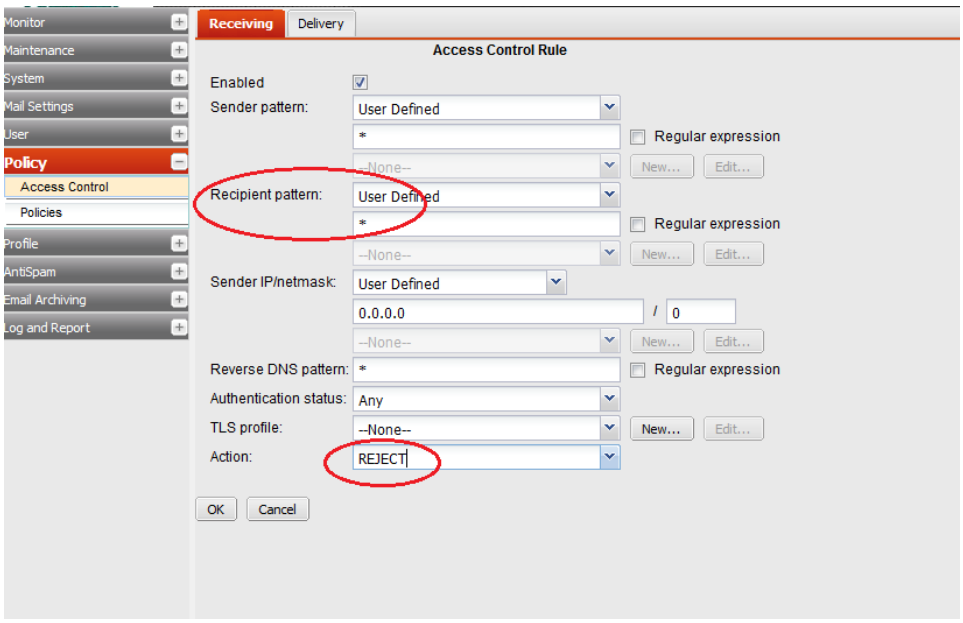
+ Đối với thành phần MTA-in là Fortimail

Vào phần Mail Settings - Domain, tạo những domain mà thiết bị MTA-in chỉ nhận email gửi đến những domain này.



Việc thiết lập xem MTA-in Fortimail chỉ nhận những email gửi đến domain nào được cấu hình trong phần Policy - Access Control.

- Nếu không có luật nào trong Access Control thì mặc định Fortimail chỉ nhận những email gửi đến domain trong phần Mail Settings - Domain. Nếu nhận được email gửi đến domain khác thì mặc định Fortimail sẽ chặn.
- Nếu có luật trong Access Control thì phải đảm bảo tạo 1 luật ở cuối cùng để chặn những email gửi đến domain khác, chú ý phần Recipient Pattern phải để là * và Action phải là Reject.



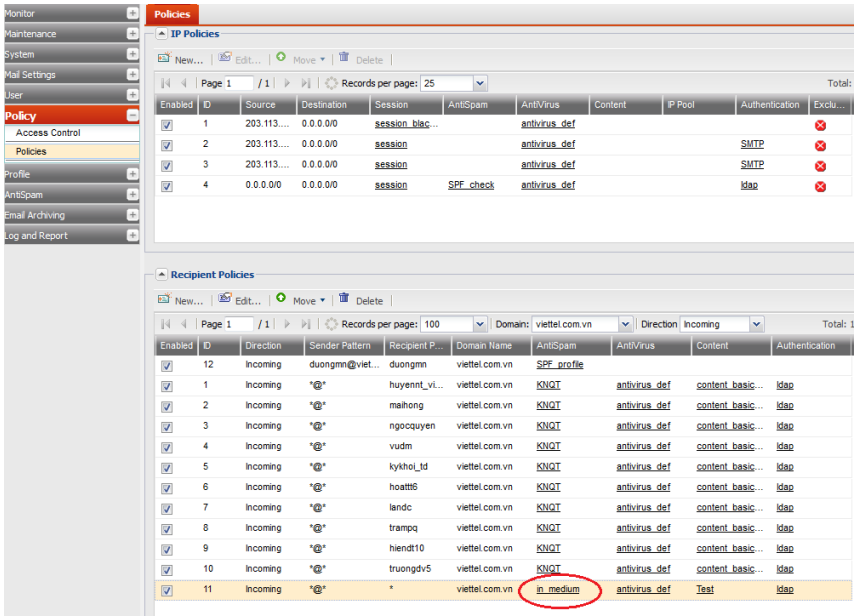
- Hoặc phải đảm bảo không có luật nào có phần Recipient Pattern là * mà Action để là RELAY.

- Cấu hình kiểm tra IP, domain blacklist (reputation) theo tổ chức uy tín trên thành phần nhận mail

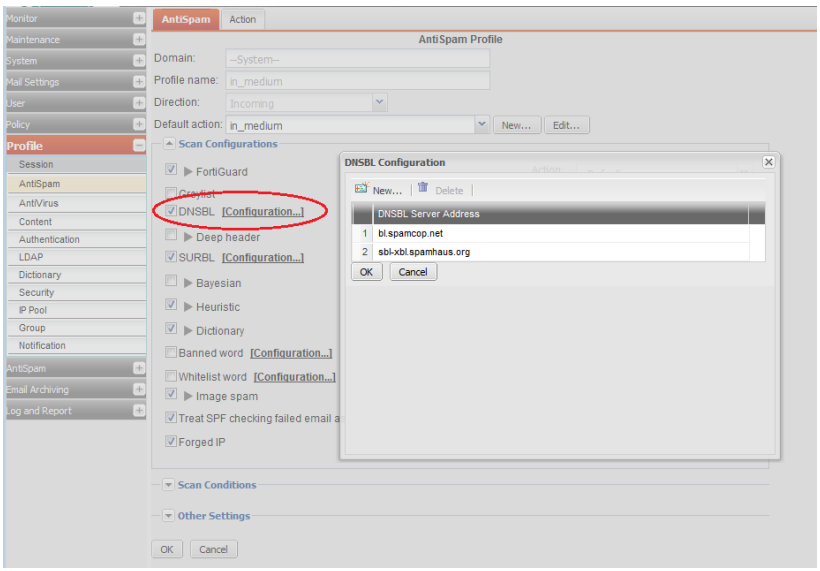
+ Đối với thành phần MTA-in là Fortimail

Sửa Antispam profile đang sử dụng hoặc nếu chưa sử dụng Antispam profile nào thì cần tạo mới (Trong Profile - AntiSpam) và áp dụng.

- Cách kiểm tra Antispam profile đang sử dụng thì vào phần Policy - Policies - Recipient Policies. Tìm kiếm theo Direction là Incomming, domain cần cấu hình profile, Receipient Pattern là *, khi đó trong mục Antispam profile sẽ hiển thị profile hiện tại đang được áp dụng hiện tại.



Trong Antispam profile cần sửa, Click DNSBL và nhập vào danh sách website chứa thông tin về danh sách IP blacklist.

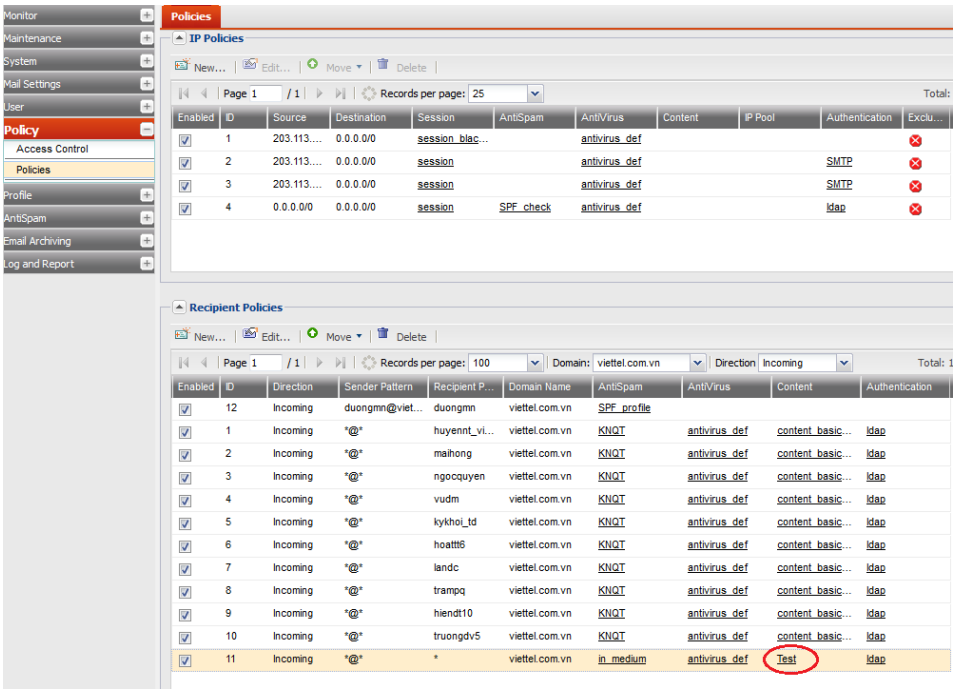


Click OK.

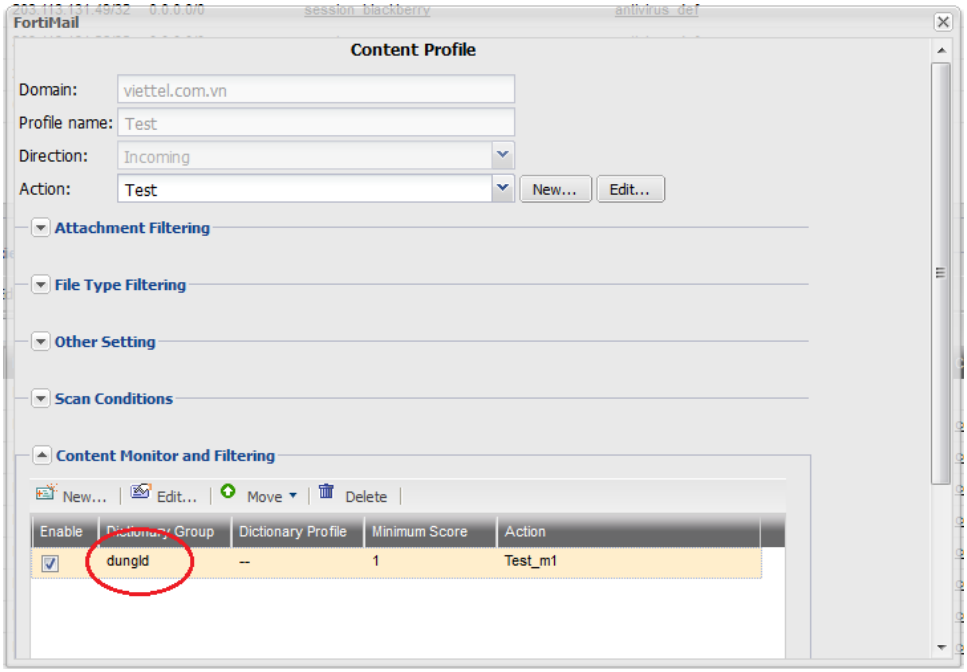
- Phải hỗ trợ cấu hình chặn lọc theo các tiêu chí: IP, domain, địa chỉ email, tiêu đề, từ khóa trong luồng mail sử dụng trực tiếp nội bộ

+ Đối với các thành phần là Fortimail

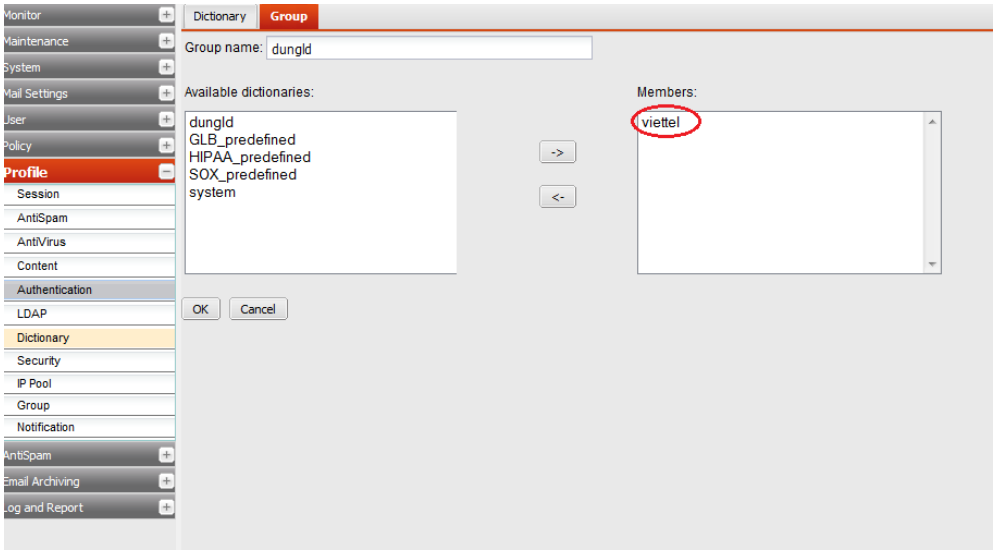
- Sửa Dictionary profile đang sử dụng hoặc nếu chưa sử dụng Dictionary profile nào thì cần tạo mới (Trong Profile - Dictionary) và áp dụng.
- Cách kiểm tra Dictionary profile đang sử dụng thì vào phần Policy - Policies - Recipient Policies. Tìm kiếm theo Direction là Incomming, domain cần cấu hình profile, Receipient Pattern là *, khi đó trong mục Content, click vào phần Content để xem thêm chi tiết.



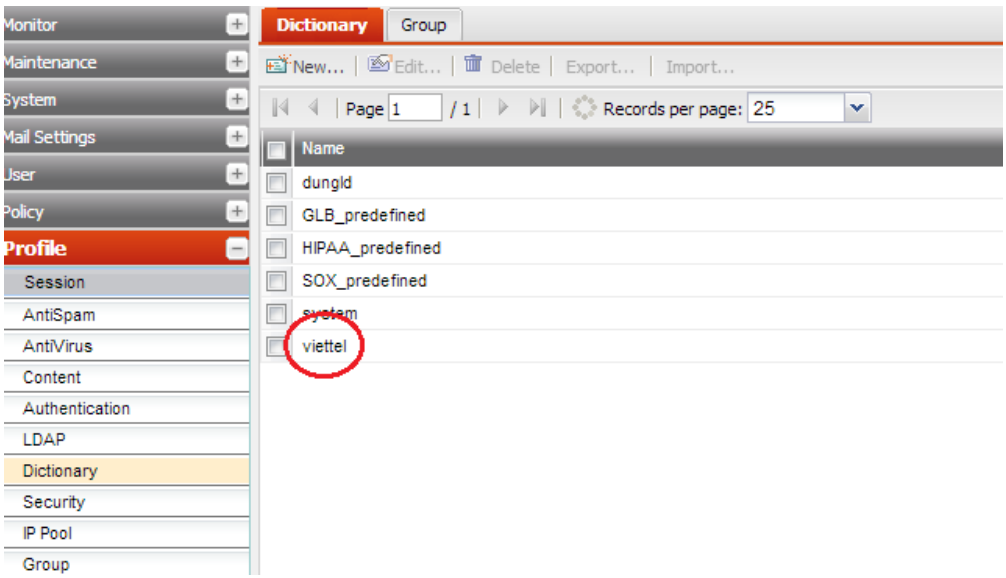
- Khi click vào phần Content đang sử dụng, trong phần Content Monitor and Filtering sẽ hiển thị Dictionary Group đang sử dụng



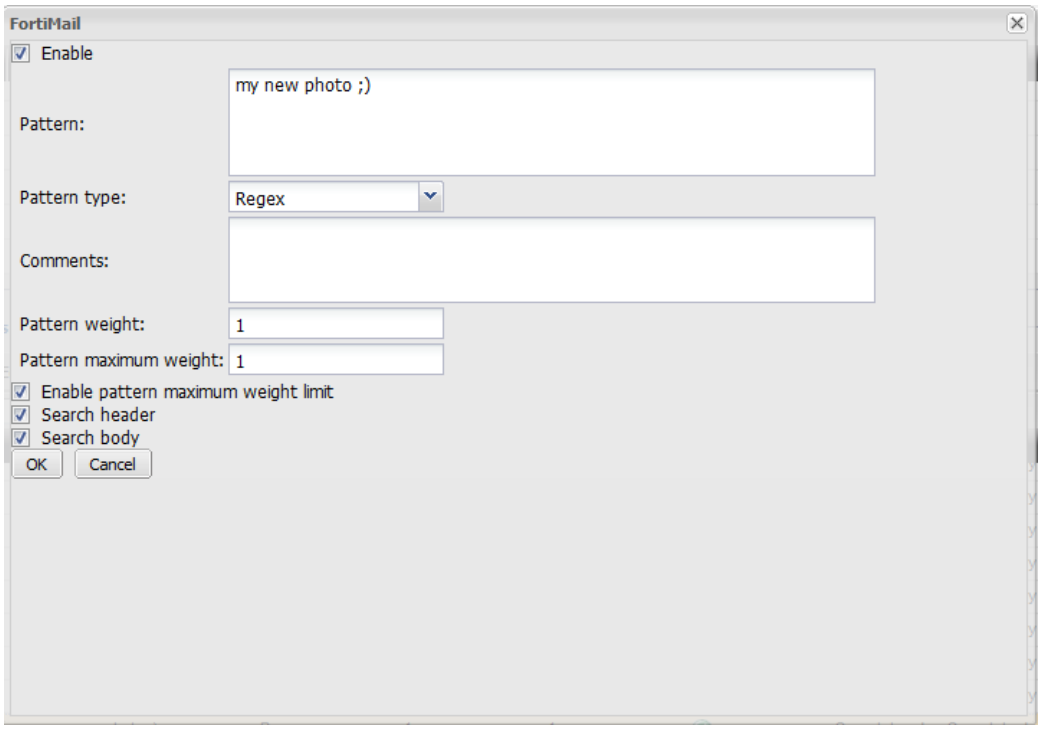
- Sau đó vào phần Profile - Dictionary - Group, chọn Group đang sử dụng, trong phần Members sẽ thấy được thư viện đang sử dụng trong group đó



- Vào tab Dictionary chọn Dictionary thuộc group đang sử dụng - click Edit để chỉnh sửa subject cần chặn.



- Trong Dictionary đang sử dụng, click New để thêm mới 1 subject cần chặn, điền nội dung subject vào phần Pattern, nếu cần chặn trong cả nội dung email thì click vào phần Search body

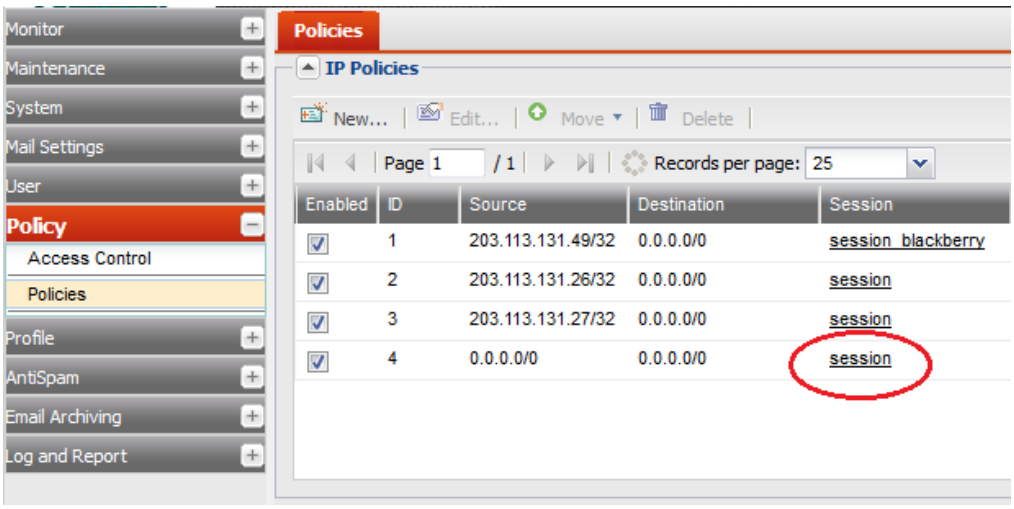


- Phải giới hạn tốc độ gửi nhận email trên các thiết bị trên thành phần gửi email MTA

+ Đối với thành phần là Fortimail

Sửa Session profile đang sử dụng hoặc nếu chưa sử dụng Session profile nào thì cần tạo mới (Trong Profile - Session) và áp dụng.

- Cách kiểm tra Session profile đang sử dụng thì vào phần Policy - Policies - IP Policies, kiểm tra Policy nào có Source là 0.0.0.0/0 khi đó trong mục Session chính là Session profile đang sử dụng.



- Trong Session Profile, sửa phần Connection Settings, chú ý các tham số:

  Restric the number of connections per client to: Giới hạn tốc độ tạo session từ 1 IP client. Ví dụ tối đa 200 session / 5 phút.

  Maximum concurrent connections for each client: Giới hạn số session đồng thời từ 1 IP Client. Ví dụ 4 session đồng thời / 1 IP.

- Cũng trong Session Profile, sửa phần SMTP Limits, chú ý tham số:

Restrict number of email per session to: Giới hạn số email tối đa có thể gửi trong 1 session. Ví dụ 10 email / 1 session.

Restric number of recipients per email to: Giới hạn trong 1 email thì có tối đa bao nhiêu người nhận. Ví dụ 150 người nhận / 1 email.

- Hỗ trợ phát hiện email spam theo nội dung (Khuyến cáo)

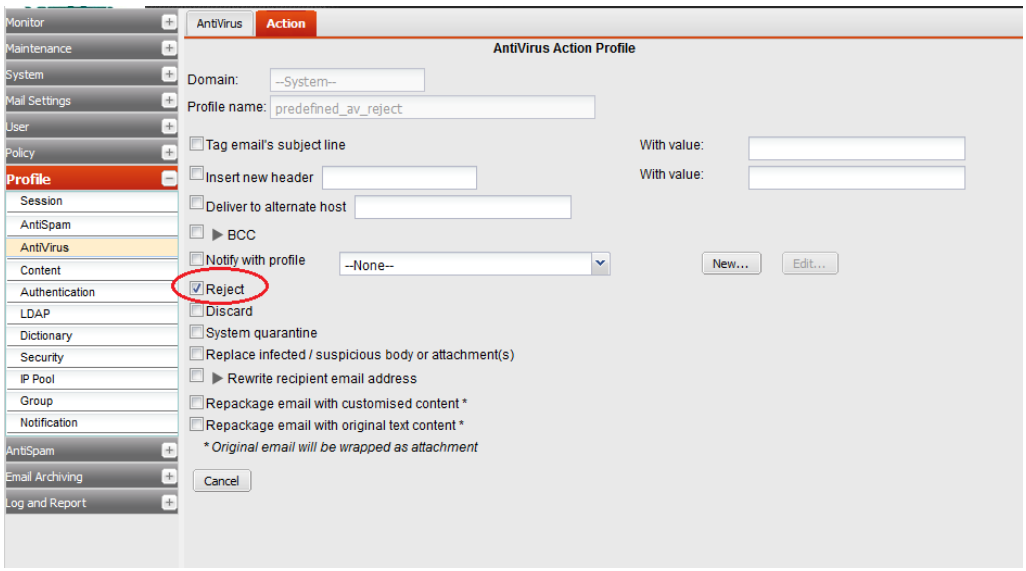
8. Yêu cầu về chống mã độc

- Toàn bộ email gửi/nhận phải được chặn lọc spam và quét virus

+ Đối với các thành phần là Fortimail hướng dẫn enable chặn lọc virus

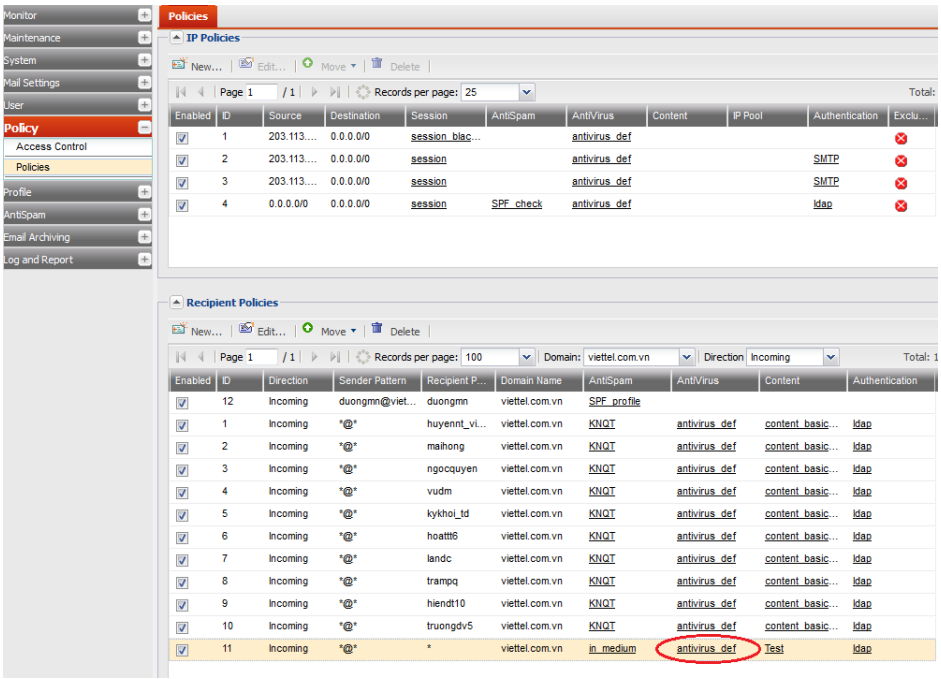
Vào Profile - Antivirus - chọn Tab Action

Nếu chưa có action là có Action là Reject thì cần tạo mới 1 action như vậy, lưu ý Action là Reject

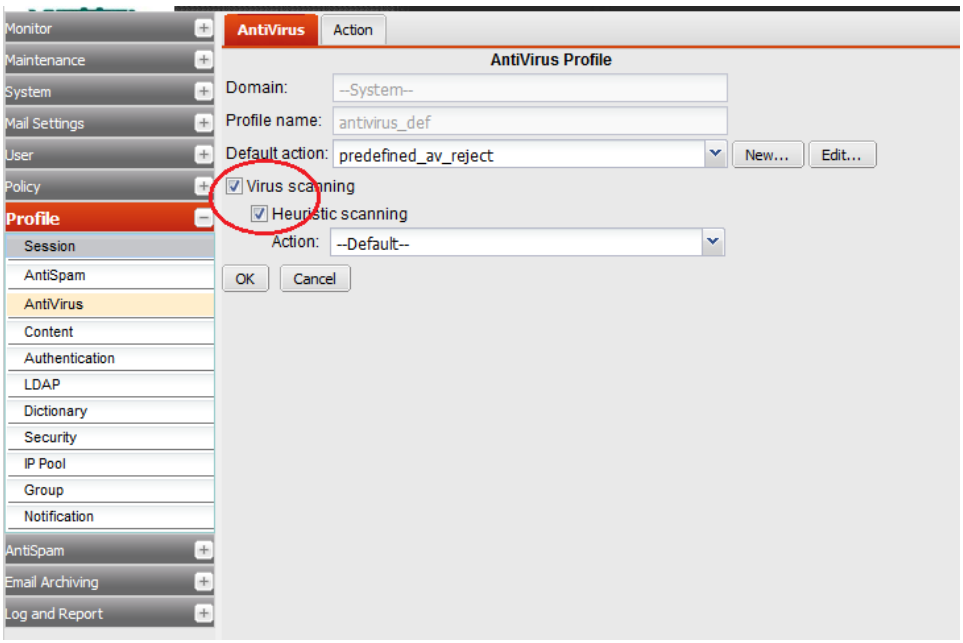


Sửa Antivirus profile đang sử dụng hoặc nếu chưa sử dụng Antivirus profile nào thì cần tạo mới (Trong Profile - Antivirus) và áp dụng.

Cách kiểm tra Antivirus profile đang sử dụng thì vào phần Policy - Policies - Recipient Policies. Tìm kiếm theo Direction là Incoming, domain cần cấu hình profile, Recipient Pattern là *, khi đó trong mục Antivirus là Profile Antivirus đang sử dụng



Trong Antivirus profile cần sửa, tích chọn Virus scanning và Heuristic scanning, trong mục Default Action chọn Action reject đã tạo.



Để cập nhật mẫu Virus thường xuyên thì vào phần Maintenance - FortiGuard, chỉnh auto update trong phần Scheduled update, tối thiểu 1 ngày / 1 lần. Có thể xem trạng thái update trong phần Last Update Attempt và Last Update Status

- Hệ thống email server cần phải có cơ chế chặn lọc mã độc, APT

Các loại mail gateway thông thường hầu hết chỉ chặn lọc các loại mã độc thông thường. Đối với các loại APT cần sử dụng các thiết bị chuyên dụng ví dụ: Email Security Gateway Viettel, Email Security for Advanced Threat Protection Fireeye, ... Khuyến cáo sử dụng bổ sung các dòng sản phẩm này tích hợp vào hệ thống email.

- Cập nhật mẫu virus hàng ngày

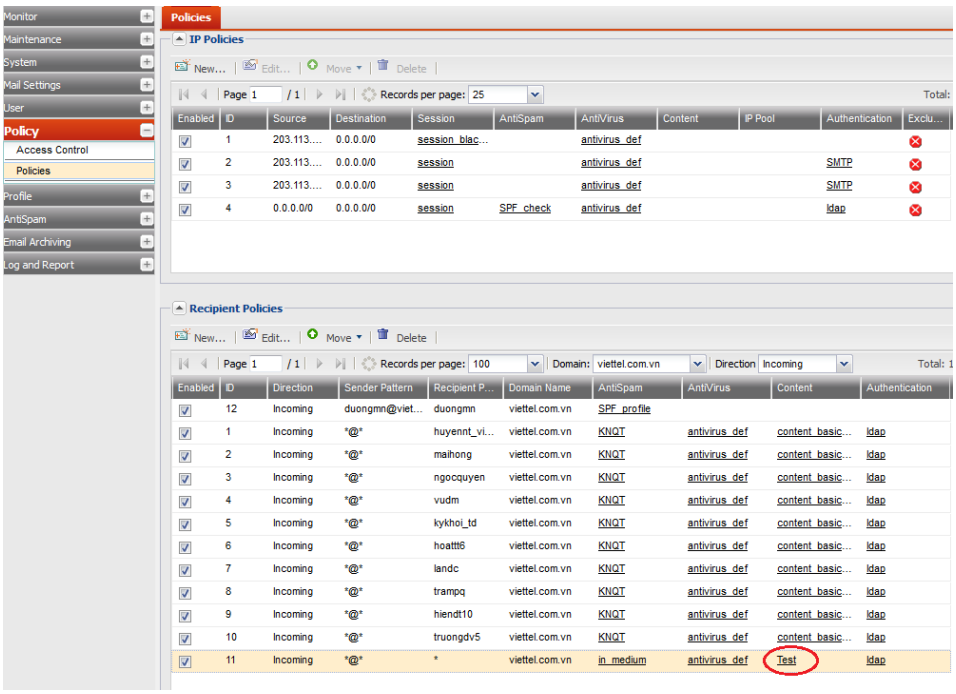
Đảm bảo license hợp lệ để cập nhật mẫu virus liên tục cho các loại mail security, mail anti APT

- Hệ thống email server không cho phép gửi nhận email có đính kèm file thực thi kể cả trong file nén: .exe, .msi, .bat, .cmd, .com, .bin, .vb, .vbs, .vbe

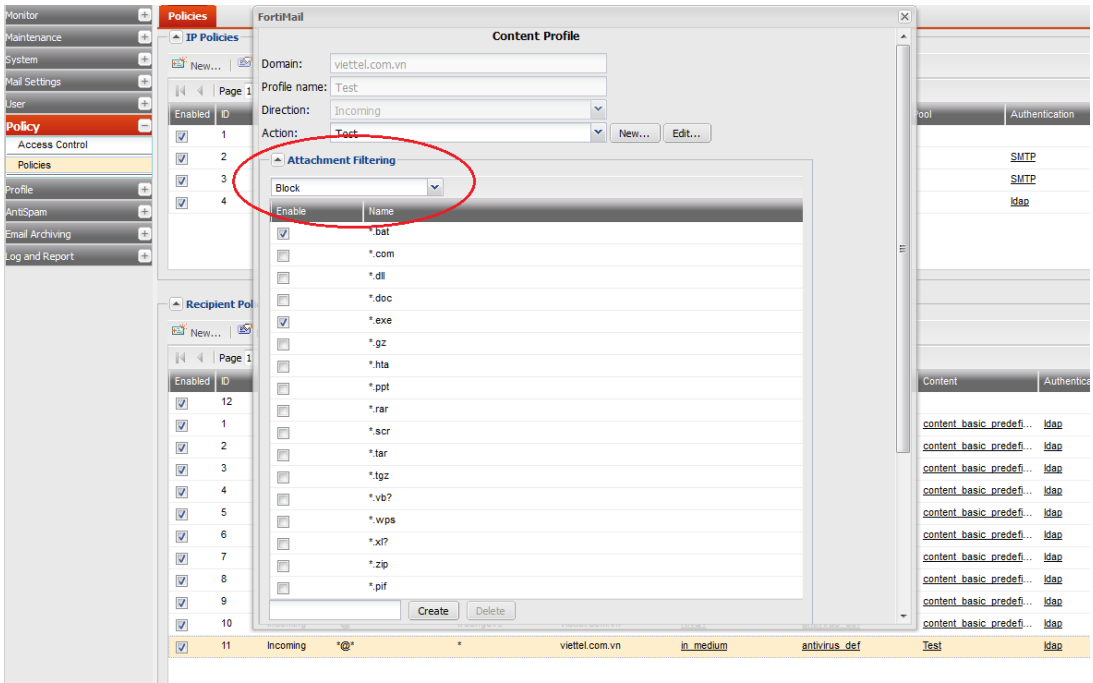
+ Đối với các thành phần là Fortimail

Sửa Content profile đang sử dụng hoặc nếu chưa sử dụng Content profile nào thì cần tạo mới (Trong Profile - Content) và áp dụng.

Cách kiểm tra Content profile đang sử dụng thì vào phần Policy - Policies - Recipient Policies. Tìm kiếm theo Direction là Incoming, domain cần cấu hình profile, Recipient Pattern là *, khi đó trong mục Content, click vào phần Content để xem thêm chi tiết.



Khi click vào phần Content đang sử dụng, trong phần Attachment Filtering chọn Block và tích chọn những định dạng file đính kèm cần chặn, nếu chưa có định dạng thì điền mới và click vào Create.



Cũng trong phần Content Profile chọn Check Archive Content để quét file nén như ZIP, PKZIP, LHA, ARJ, RAR và chọn Max Level of Compression là 5.

9. Yêu cầu về xác thực đa nhân tố khi sử dụng email (Khuyến cáo)

- Phải xác thực đa nhân tố khi người dùng sử dụng email qua web mail

- Đối với ứng dụng email client không hỗ trợ xác thực đa nhân tố như: Outlook, thunderbird, email client trên điện thoại, ... thì sử dụng cơ chế App-specific passwords (App passwords)

Hiện tại chỉ có 1 số sản phẩm hỗ trợ tính năng này: Zimbra. Riêng Exchange chỉ hỗ trợ ở bản Cloud (365) không hỗ trợ ở bản On-Primes

10.Chống rà quét mật khẩu trong luồng mail nội bộ

- Đối với đăng nhập qua web mail nội bộ: Nếu 1 account đăng nhập sai 5 lần liên tục thì sẽ yêu cầu nhập captcha

+ Tính năng mặc định của hầu hết các loại Webmail: Exchange, Zimbra, ...

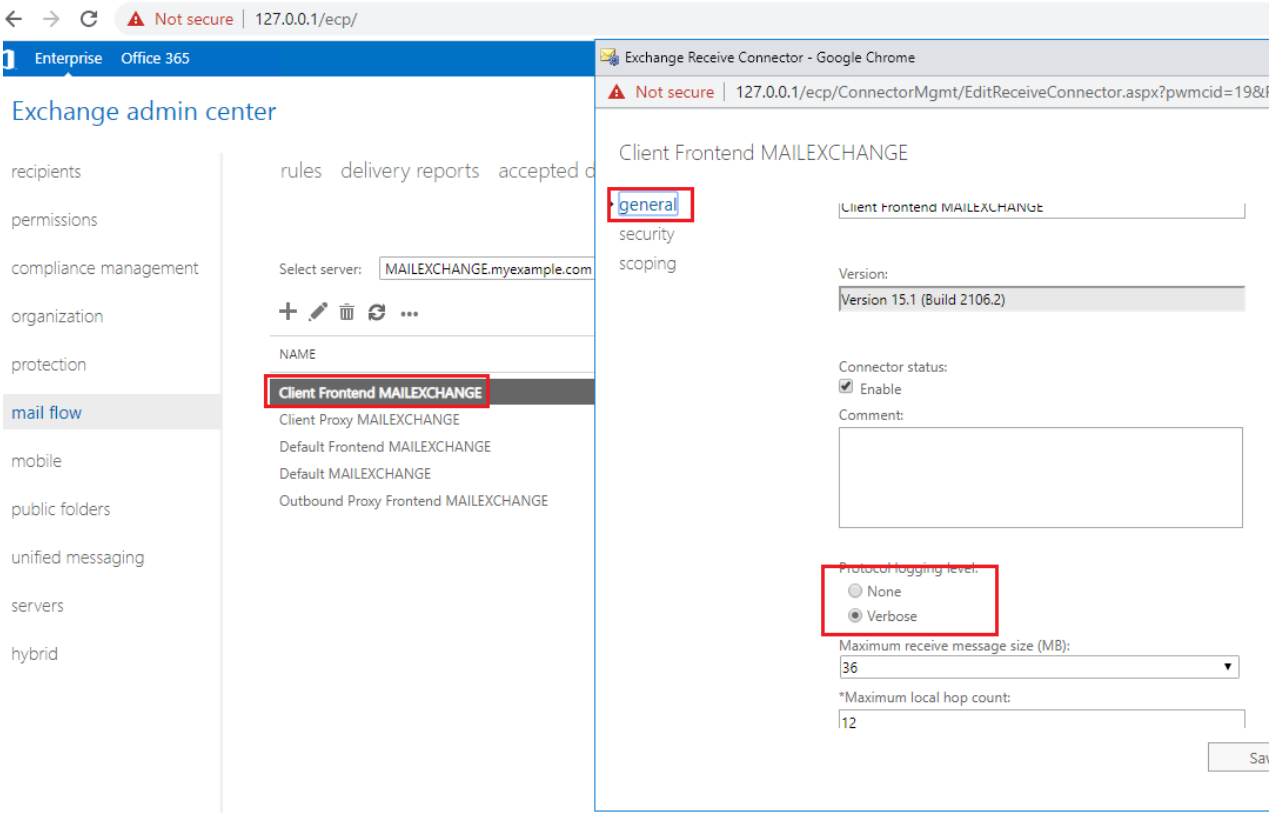
- Đối tự động block tài khoản nếu nhập sai quá nhiều lần

+ Đối với email server exchange tính năng này được cấu hình trên GPO cấu hình trên Active Directory.

11.Cấu hình log truy vết hệ thống email

- Hướng dẫn cấu hình enable Protocol log trên Exchange server

+ Vào EAD của server mail exchange. Mail flow -> Receive Connector. Đối với mỗi connector nhận email cần auth vào phần General -> Protocol login level -> Tích chọn verbose -> Chọn Save để lưu lại



- Tất cả các log được lưu tập trung, lưu tối thiểu 3 tháng

+ Sử dụng agent security để đẩy log về các loại SIEM hoặc Log Center System để lưu trữ trong thời gian dài (Tối thiểu 3 tháng)

12.Yêu cầu về việc đánh giá ATTT định kỳ

Việc đánh giá ATTT cho hệ thống Email phải được thực hiện định kỳ theo quy định của đơn vị phụ trách ATTT.

Phụ lục 10.
HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HỆ THỐNG ACTIVE DIRECTORY

1. Yêu cầu về việc cài đặt hệ thống Active Directory (AD) an toàn

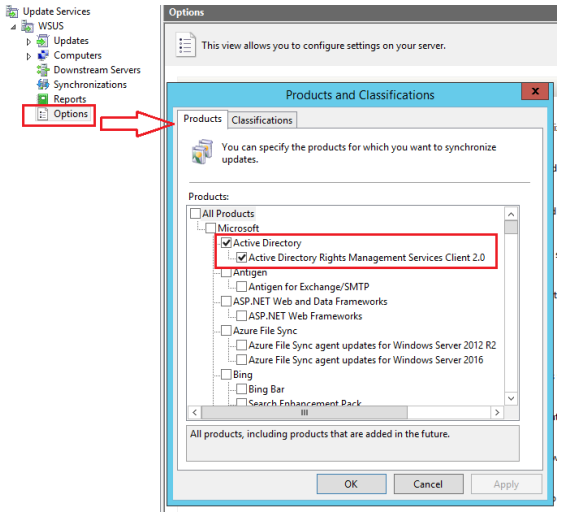
1.1. Cài đặt hệ điều hành an toàn

Xem hướng dẫn Quy tắc cấu hình ATTT cho hệ điều hành máy chủ.

1.2. Cài đặt Hệ thống active directory an toàn

- Sau khi cài đặt máy chủ AD phải update các bản vá lỗi thường xuyên.

Chú ý: Đối với trường hợp sử dụng WSUS phải enable update các bản cập nhật Security cho Active Directory. Trên máy chủ WSUS cấu hình như sau.



2. Yêu cầu môi trường vận hành an toàn

- Máy sử dụng để remote vào vận hành hệ thống Active Directory phải là 1 máy riêng (có thể là máy ảo, VDI hoặc máy PC). Máy tính này phải đáp ứng các yêu cầu sau.

+ Đáp ứng đầy đủ các tiêu chuẩn ATTT của tổ chức cho máy người dùng cuối.

+ Không sử dụng cho các mục đích thông thường như: Truy cập internet, check email, xoạn thảo/đọc các văn bản dạng Word, PDF.

+ Có thể sử dụng 1 máy VDI để remote và đặt lịch restore lại trạng thái sạch định kỳ hàng ngày.

3. Yêu cầu bảo vệ tài khoản đặc quyền, nhóm đặc quyền

- Yêu cầu không sử dụng tài khoản thuộc nhóm có quyền cao trong AD trong một số công việc không yêu cầu quyền đặc biệt.

+ Các tài khoản có quyền cao trong AD là các tài khoản thuộc nhóm Domain Admins, Schema Admins, Enterprise Admins và tài khoản Administrator AD.

+ Không sử dụng các tài khoản thuộc nhóm có quyền cao để làm tài khoản Email, tài khoản kết nối LDAP xác thực vào các hệ thống khác.

+ Các tài khoản sử dụng vận hành phải được tách ra không được trùng với tài khoản đăng nhập máy tính hàng ngày.

- Yêu cầu chỉ sử dụng tài khoản thuộc nhóm có quyền cao trong việc xử lý sự cố hoặc cài đặt các hệ thống yêu cầu quyền tương ứng

+ Trường hợp cài đặt các hệ thống yêu cầu quyền đặc biệt (VD: exchange) thì chỉ sử dụng tài khoản quyền cao trong quá trình cài đặt, không dùng trong vận hành hàng ngày. Sau khi cài đặt tạo 1 account thường (Normal Users) gán quyền quản trị cho account này để vận hành hàng ngày.

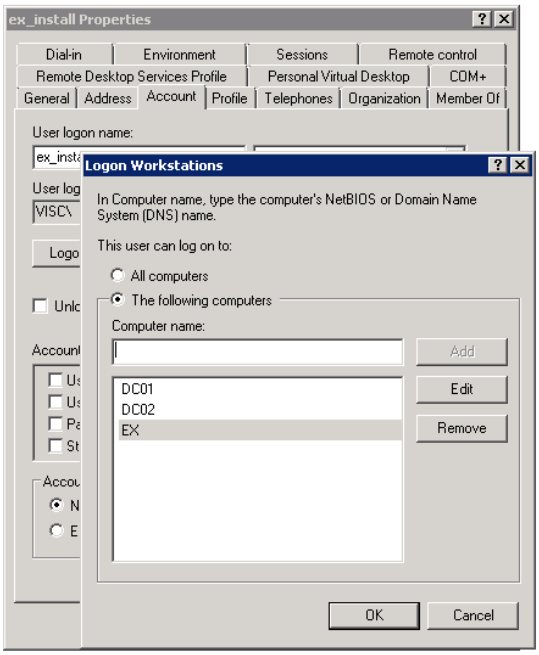
+ Các bước quá trình cài đặt sử dụng tài khoản có quyền cao phải tuân thủ trình tự sau: Thiết lập log on to -> Cài đặt -> Thu hồi log on to.

Ví dụ: ở đây là sử dụng tài khoản ex_install để cài đặt Exchange email server tên là EX.

B1. Thiết lập log on to ta chọn account ex_install

Tạo account ex_install, thiết lập các quyền cần thiết để cài đặt.

Trong Active Directory Users and Groups -> chọn Tab Account -> Log on to



Chọn The following computers và điền vào các máy gồm: các DC (ở đây là DC01 và DC02) và máy muốn cho account login vào cài đặt EX.

B2: Cài đặt hệ thống.

B3: Thu hồi log on to: Làm như B1 nhưng remove máy EX đi.

+ Trường hợp bắt buộc phải sử dụng account có quyền cao để xử lý thì phải thiết lập logon to. Làm như trên nhưng bỏ B3.

- Yêu cầu rà soát các account thuộc nhóm có quyền cao. Loại bỏ các tài khoản không sử dụng

+ Danh sách user của 1 số nhóm có đặc quyền cao mặc định sau khi cài xong Active Directory.

Nhóm	**Danh sách member mặc định**
Domain Admins	Administrator
Schema Admins	Administrator
Enterprise Admins	Administrator
Administrators	Administrators, Domain Admins, Enterprise Admins,

Dựa vào danh sách mặc định trên ta sẽ loại bỏ đi các account quản trị thêm vào không sử dụng.

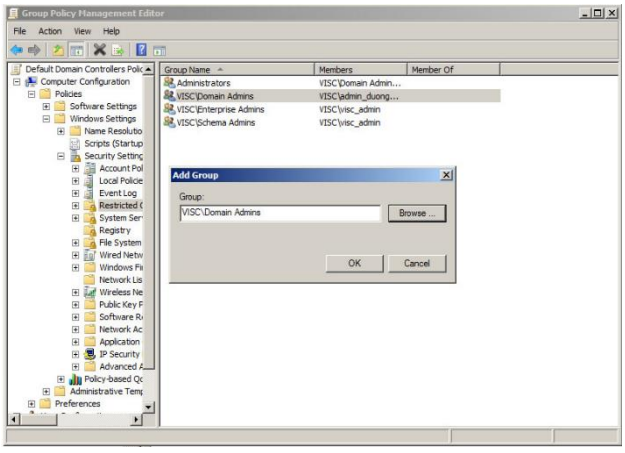
- Yêu cầu giới hạn các tài khoản thuộc các nhóm có quyền cao trên AD. (Thiết lập trên Default Domain Controller Group policy.)

+ Sử dụng tính năng Restricted Group trong Group Policy để giới hạn các account thuộc nhóm người dùng có đặc quyền cao

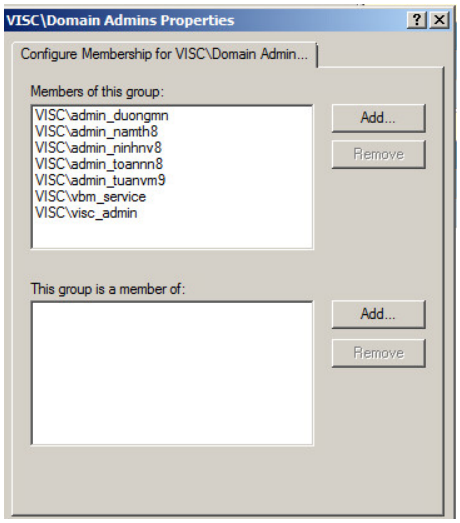
Sử dụng công cụ Group Policy Management để edit Default Domain Controller Policy

Vào phần *Computer Configuration -> Windows Setting -> Security Setting -> Restricted Group*. Chuột phải chọn New

Trong hộp thoại hiện lên Phần Add Group thêm vào Group định giới hạn.



Phần **Member of this group** là danh sách các user sẽ giới hạn thuộc group này.



Thực hiện giới hạn user với các nhóm đặc quyền

- Yêu cầu sử dụng tài khoản thường (Domain users) được ủy quyền để thực hiện một số tác vụ hàng ngày.

+ Sử dụng tài khoản thường để join/unjoin máy tính.

+ Tạo 1 tài khoản/nhóm tài khoản có quyền administrator local để cài đặt phần mềm cho máy tính người dùng.

4. Chống tấn công leo thang trên hệ thống AD

- Giới hạn các tài khoản Administrator (AD) không có quyền đăng nhập từ xa đến các máy chủ Domain Controller

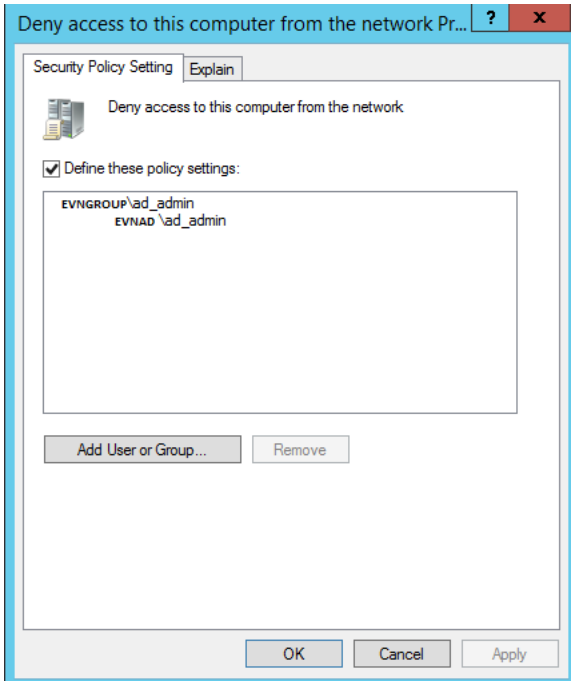
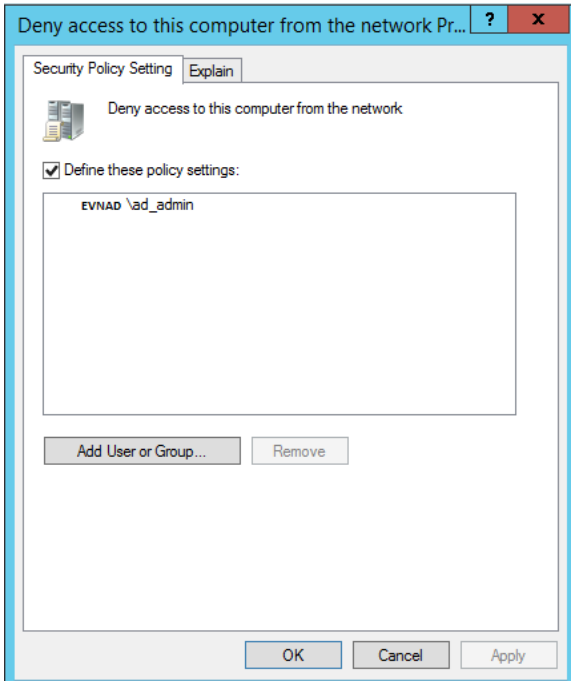
+ Tạo mới policy của Domain Controller:

+ Vào Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments. Chỉnh sửa các giá trị sau:

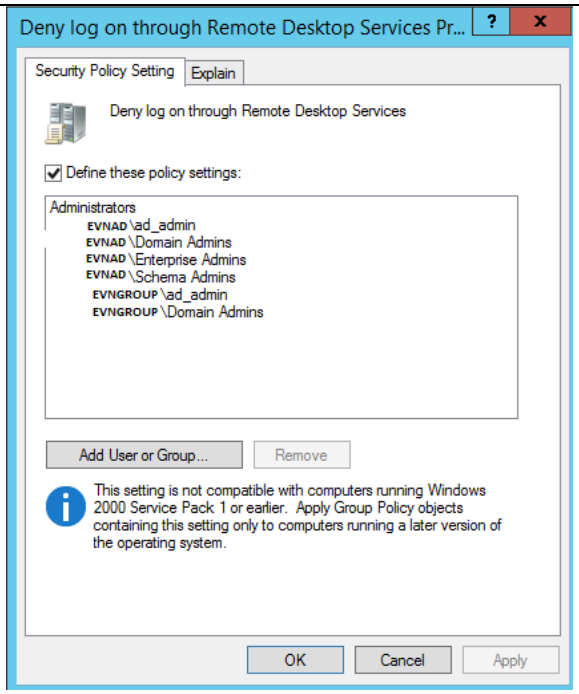
+ **Lưu ý:**

  - Ở mục 4: Deny log on locally không định nghĩa.
  - Chỉ áp dụng đối với tài khoản Administrator (AD), không áp dụng với các tài khoản thuộc nhóm Domain Admins, Enterprise Admins, Schema Admins.

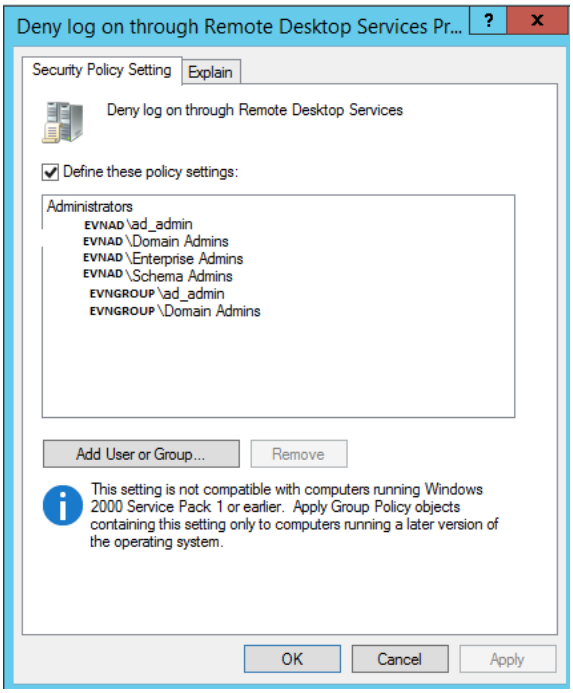
STT	Policy	Value
1	Deny access to this computer from the network	DOMAIN\Administrator: Là tài khoản administrator mặc định của DOMAIN. Nếu đã đổi tên tài khoản này thì nhập tên tài khoản sau khi đổi (ví dụ EVNGROUP\AD_Admin). Lưu ý: Trong trường hợp AD của tổ chức theo mô hình subdomain thì:

		- Trên GPO của các máy chủ DC thuộc AD sub: add thêm cả tài khoản administrator của AD root(Ví dụ là EVNAD\AD_Admin).  - Trên GPO của các máy chủ DC thuộc AD root: Chỉ add tài khoản administrator của AD root. 
2	Deny log on as a batch job	**Như mục 1**

3	Deny log on as a service	**Như mục 1**
4	Deny log on locally	**Not defined**
5	Deny log on through Remote Desktop Services	**Như mục 1 nhưng thêm các nhóm sau:** Administrators: Là nhóm Administrators mặc định của AD. DOMAIN\Domain Admins: Là nhóm Domain Admins (Ví dụ EVNGROUP\Domain Admins). Lưu ý Trong trường hợp AD của tổ chức theo mô hình subdomain thì: - Trên GPO của các máy chủ DC của AD sub: add thêm cả nhóm Domain Admins của AD root (Ví dụ là EVNAD\Domain Admins). - Trên GPO của các máy chủ DC của AD root: chỉ add nhóm Domain Admins của AD root chứ không add nhóm Domain Admins của AD sub. DOMAIN\Enterprise Admins: Là nhóm Enterprise Admins của domain. Lưu ý Trong trường hợp AD của tổ chức theo mô hình subdomain thì chỉ add nhóm Enterprise Admins của AD root (Ví dụ là EVNAD\Enterprise Admins) trên cả GPO cho các máy chủ DC của AD root và GPO của các máy chủ DC của AD sub. DOMAIN\Schema Admins: Tương tự nhóm Enterprise Admins. Lưu ý Trong trường hợp AD của tổ chức theo mô hình subdomain thì chỉ add nhóm Schema Admins của AD root (Ví dụ là EVNAD\ Schema Admins) trên cả GPO cho các máy chủ DC của AD root và GPO của các máy chủ DC của AD sub. Ví dụ GPO trên AD sub:

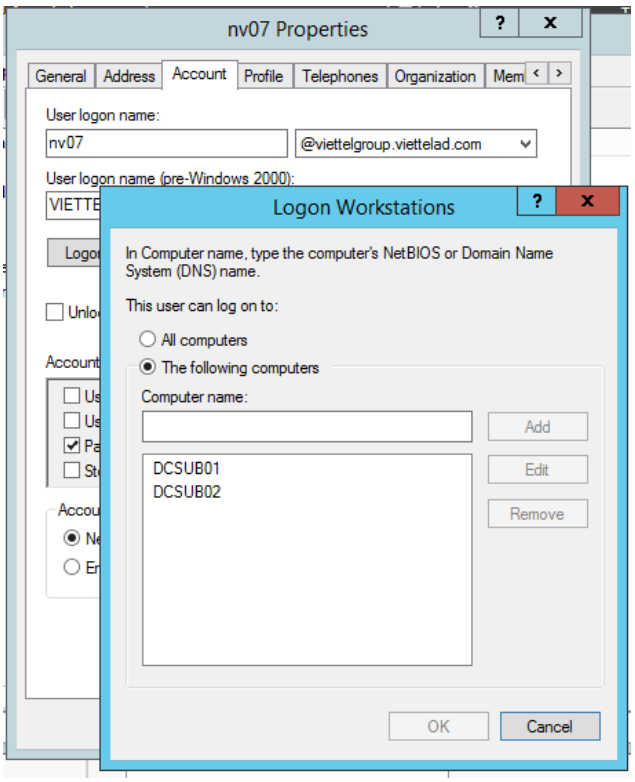


Ví dụ GPO trên AD root:



- Giới hạn Logon to đối với các tài khoản thuộc nhóm Domain Admins, Enterprise Admins, Schema Admins

- Đối với các tài khoản thuộc nhóm Domain Admins, Enterprise Admins, Schema Admins thì phải giới hạn logon to chỉ trên các máy DC



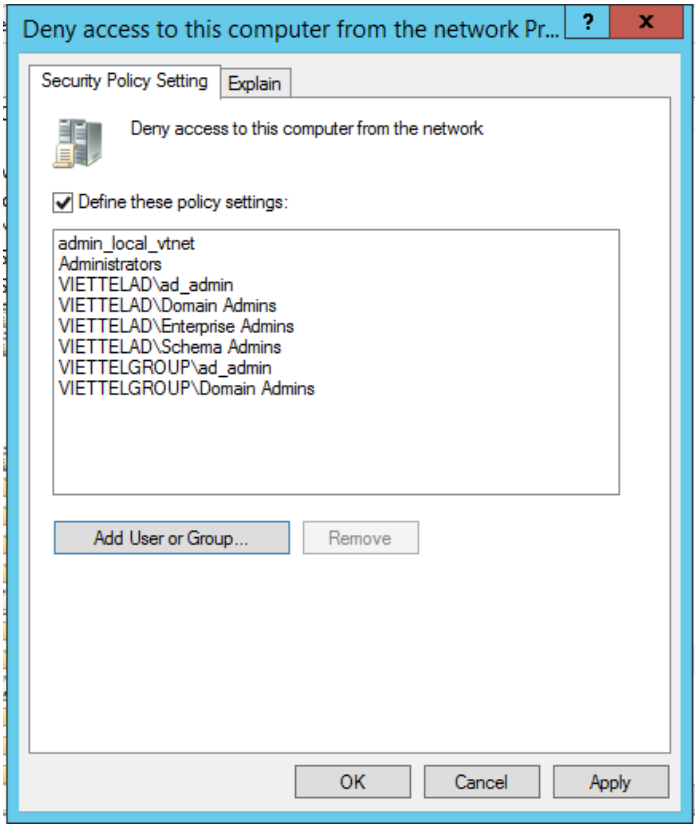
5. Chống tấn công chéo (ngang hàng) trong hệ thống AD

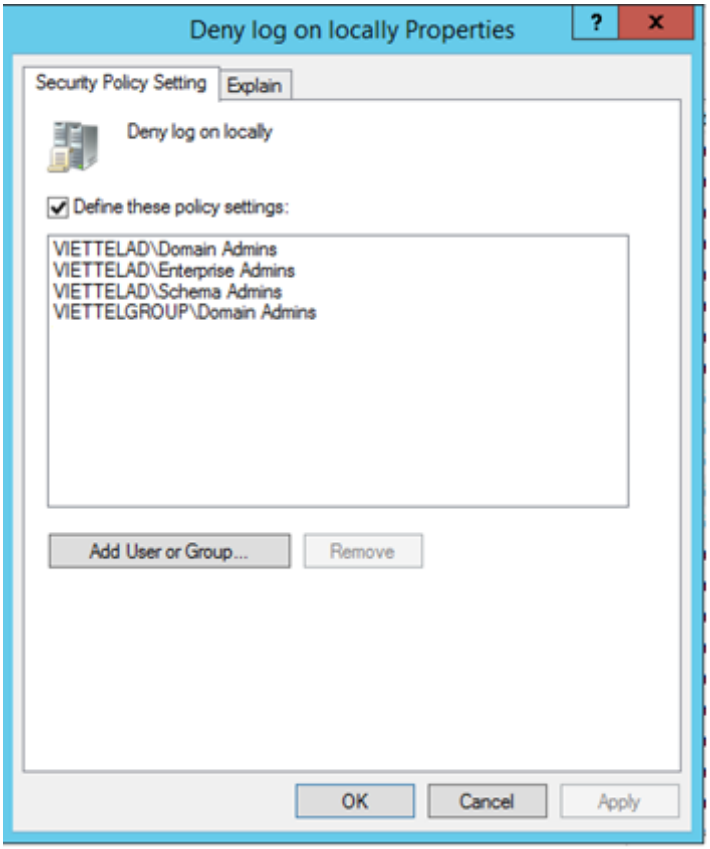
- Giới hạn các tài khoản quản trị của domain không có quyền đăng nhập trên máy tính người dùng bình thường và member server.

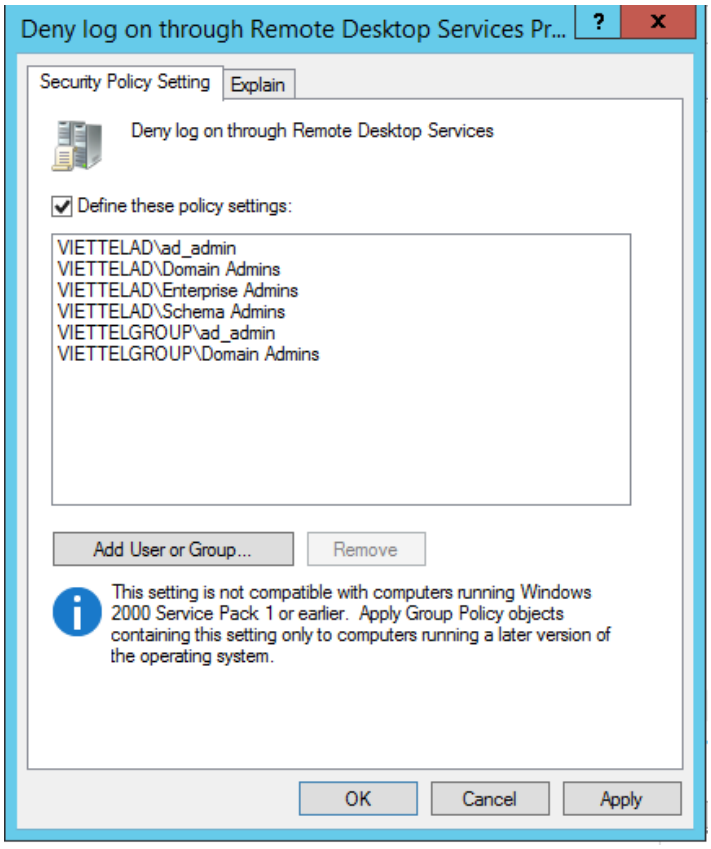
+ Tạo hoặc sửa 1 GPO chứa các máy tính người dùng và member server

+ Vào Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments. Chỉnh sửa các giá trị sau:

STT	Policy	Value
1	Deny access to this computer from the network	DOMAIN\Administrator: Là tài khoản administrator mặc định của DOMAIN. Nếu đã đổi tên tài khoản này thì nhập tên tài khoản sau khi đổi (ví dụ EVNGROUP\AD_Admin). Lưu ý Trong trường hợp AD của tổ chức theo mô hình subdomain thì add thêm cả tài khoản administrator của AD root(Ví dụ là EVNAD\AD_Admin). DOMAIN\Domain Admins: Là nhóm Domain Admins (Ví dụ EVNGROUP\Domain Admins). Lưu ý Trong trường hợp AD của tổ chức theo mô hình subdomain thì add thêm cả nhóm Domain Admins của AD root (Ví dụ là EVNAD\Domain Admins). DOMAIN\Enterprise Admins: Là nhóm Enterprise Admins của domain. Lưu ý Trong

		trường hợp AD của tổ chức theo mô hình subdomain thì chỉ add nhóm Enterprise Admins của AD root (Ví dụ là EVNAD\Enterprise Admins) vì AD sub không có nhóm Enterprise Admins. DOMAIN\Schema Admins: Tương tự nhóm Enterprise Admins. Nếu hoạt động theo mô hình subdomain thì chỉ add nhóm Schema Admins của AD root vì AD sub không có nhóm Schema Admins. Tài khoản Administrator local: Nếu đã đổi tên thì nhập tên tài khoản sau khi đã đổi. Nhóm Administrators: Nhóm Administrators local trên máy người dùng, member server. 
2	Deny log on as a batch job	**Như mục 1**
3	Deny log on as a service	**Như mục 1**
4	Deny log on locally	DOMAIN\Domain Admins: Là nhóm Domain Admins (Ví dụ EVNGROUP\Domain Admins). Lưu ý Trong trường hợp AD của tổ chức theo mô hình subdomain thì add thêm cả

		nhóm Domain Admins của AD root (Ví dụ là EVNAD\Domain Admins). DOMAIN\Enterprise Admins: Là nhóm Enterprise Admins của domain. Lưu ý Trong trường hợp AD của tổ chức theo mô hình subdomain thì chỉ add nhóm Enterprise Admins của AD root (Ví dụ là EVNAD\Enterprise Admins) vì AD sub không có nhóm Enterprise Admins. DOMAIN\Schema Admins: Tương tự nhóm Enterprise Admins. Nếu hoạt động theo mô hình subdomain thì chỉ add nhóm Schema Admins của AD root vì AD sub không có nhóm Schema Admins. 
5	Deny log on through Remote Desktop Services	DOMAIN\Administrator: Là tài khoản administrator mặc định của DOMAIN. Nếu đã đổi tên tài khoản này thì nhập tên tài khoản sau khi đổi (ví dụ EVNGROUP\AD_Admin). Lưu ý Trong trường hợp AD của tổ chức theo mô hình subdomain thì add thêm cả tài khoản administrator của AD root (Ví dụ là EVNAD\AD_Admin).

		DOMAIN\Domain Admins: Là nhóm Domain Admins (Ví dụ EVNGROUP\Domain Admins). Lưu ý Trong trường hợp AD của tổ chức theo mô hình subdomain thì add thêm cả nhóm Domain Admins của AD root (Ví dụ là EVNAD\Domain Admins). DOMAIN\Enterprise Admins: Là nhóm Enterprise Admins của domain. Lưu ý Trong trường hợp AD của tổ chức theo mô hình subdomain thì chỉ add nhóm Enterprise Admins của AD root (Ví dụ là EVNAD\Enterprise Admins) vì AD sub không có nhóm Enterprise Admins. DOMAIN\Schema Admins: Tương tự nhóm Enterprise Admins. Nếu hoạt động theo mô hình subdomain thì chỉ add nhóm Schema Admins của AD root vì AD sub không có nhóm Schema Admins. 

6. Sao lưu log đăng nhập

- Thiết lập theo phần cấu hình log của Guideline theo hệ điều hành máy chủ
- Đẩy log về hệ thống SIEM của tổ chức

7. Đánh giá ATTT định kỳ

- Đưa các yêu cầu đánh giá ATTT định kỳ vào chính sách ATTT của tổ chức định kỳ.

Phụ lục 11.
HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HỆ THỐNG WEB SECURITY BLUECOAT

1. Yêu cầu về việc cài đặt hệ thống proxy server an toàn

- Đảm bảo License của hệ thống phải còn thời hạn sử dụng

Truy cập vào portal, **System Administration** > **Feature Keys** check thời hạn còn lại ở phần Time Remaining

Feature Keys

Feature Keys for Serial Number: 42071BC5FF78DE9C222D-C2FBD701AD99

Description	Status	Time Remaining	Expiration Date
File Reputation	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
File Analysis	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
IronPort Image Analysis	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
IronPort Anti-Spam	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
Outbreak Filters	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
Cloudmark Service Provider Edition	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
Bounce Verification	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
Incoming Mail Handling	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
Intelligent Multi-Scan	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
IronPort Email Encryption	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
RSA Email Data Loss Prevention	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
Sophos Anti-Virus	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)
McAfee	Dormant	314 days	12 May 2015 20:10 (GMT +00:00)

Pending Activation

No feature key activations are pending.

Check for New Keys

Feature Activation

Feature Key:

Submit Key

- Đảm bảo phiên bản OS của hệ thống không tồn tại các lỗ hổng CVE

Truy cập vào portal, lựa chọn phần **Monitor> System Status** để kiểm tra Version của Software của hệ thống

System Status

Mail System Status		Version Information	
System Status:	Online	Model:	C600V
Status as of:	25 Oct 2018 08:29 (GMT +00:00)	Operating System:	9.8.1-015
Up Since:	24 Oct 2018 11:22 (GMT +00:00) (21h 7m 25s)	Build Date:	05 Jun 2017 00:00 (GMT +00:00)
		Install Date:	24 Oct 2018 11:22 (GMT +00:00)
Oldest Message:	No Messages waiting for delivery	Serial Number:	422DF476E2680FE9CFAE-D347A35D69B1

2. Yêu cầu môi trường vận hành an toàn

- Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho máy người dùng cuối để vận hành các hệ thống quan trọng như AD, Proxy, Email. Khuyến nghị sử dụng máy tính VDI có chức năng tự động reset về trạng thái sạch để quản trị các máy chủ tập trung tại đơn vị

- Các máy riêng không dùng để sử dụng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MS Office/pdf) chỉ sử dụng để vận hành hệ thống

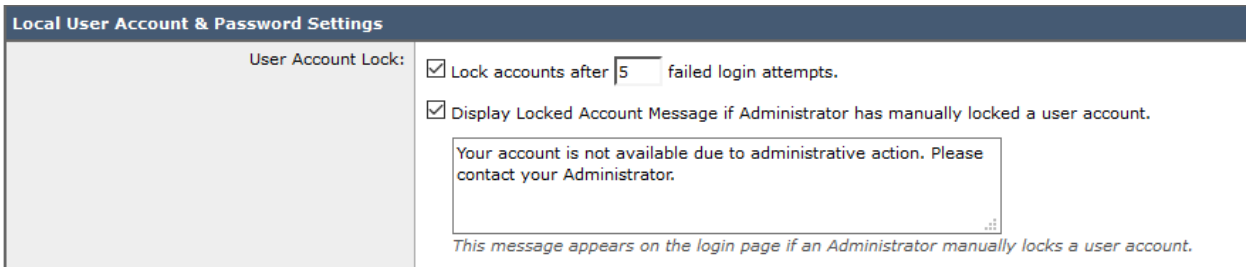
3. Yêu cầu về thiết lập hệ thống proxy

- Thiết lập trên các thiết bị network. Không nằm trong phạm vị tài liệu này

4. Yêu cầu về giới hạn đăng nhập và chính sách mật khẩu

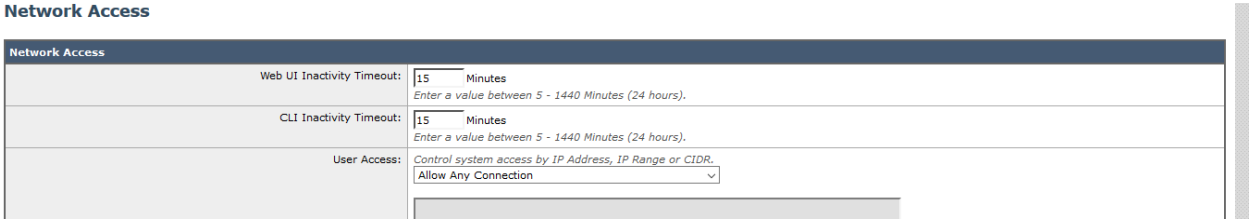
- Có giới hạn số lần nhập password không cho phép nhập sai quá 5 lần

Truy cập vào portal, **System Administration > User >** phần **Local User Account & Password Settings** click vào **Edit Settings** > ở phần **User Account Lock** tích vào 2 ô như bên dưới và đặt số lần đăng nhập sai là 5



- Có giới hạn thời gian time-out của phiên kết nối quản trị tối đa là 15 phút

Truy cập vào portal, **System Administration > Network Access >** click vào **Edit Settings** > ở phần **Web UI Inactivity Timeout** và **CLI Inactivity Timeout** điền thành 15 như ảnh và **Submit**



- Yêu cầu chính sách mật khẩu

+ Tất cả các tài khoản phải có mật khẩu.

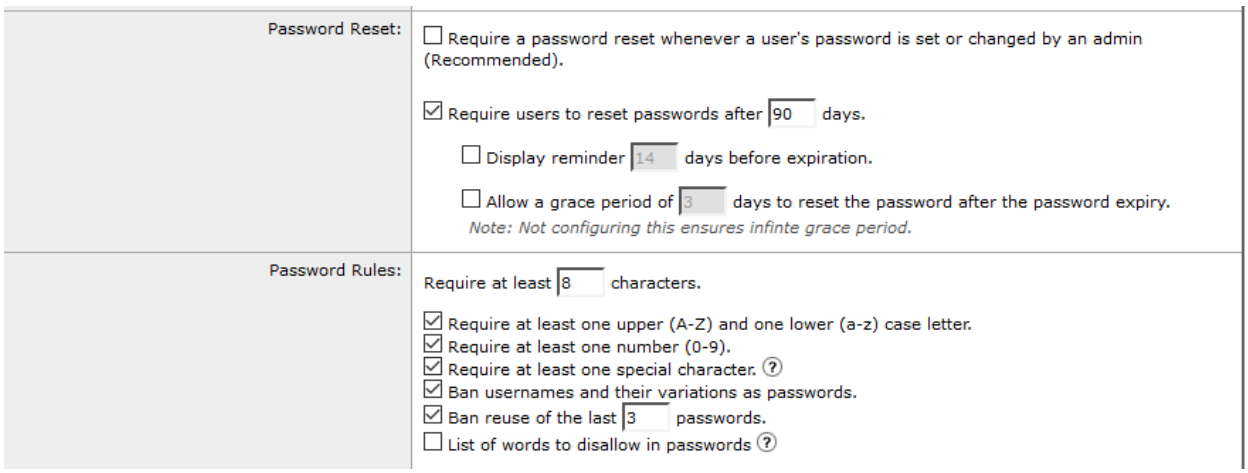
+ Mật khẩu có độ dài tối thiểu 10 ký tự.

+ Mật khẩu bao gồm tối thiểu 3 trong 4 loại ký tự sau: chữ cái viết hoa (A - Z); chữ cái viết thường (a - z); chữ số (0 - 9); các ký tự khác trên bàn phím máy tính (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /) và dấu cách.

+ Mật khẩu không chứa tên tài khoản.

- Thời gian hiệu lực của mật khẩu đối với tài khoản cá nhân tối đa là 90 ngày.

Để thiết lập rule cho mật khẩu, truy cập vào portal, **System Administration > User >** phần **Local User Account & Password Settings** click vào **Edit Settings** > ở phần **Password Reset** và **Password Rules** tích và điền các thông số như bên dưới



Add account mới hoặc edit chỉnh lại password

5. Yêu cầu cấu hình đồng bộ thời gian

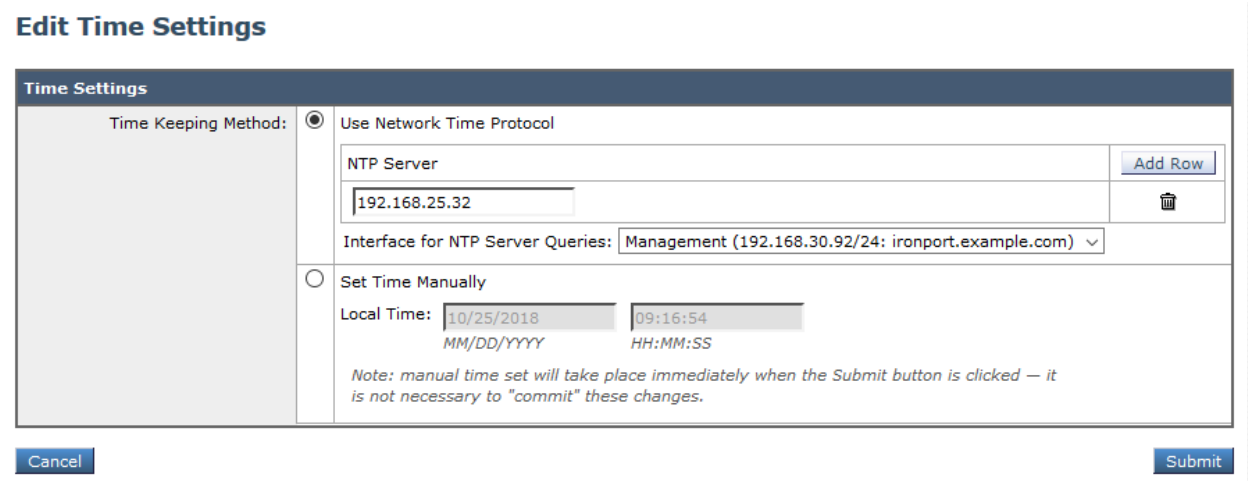
- Có cấu hình cập nhật thời gian theo giao thức NTP tới NTP Server

Chỉnh time zone cho thiết bị vào phần **System Administration > Time zone** > click vào **Edit Settings ..**> Điều chỉnh Time zone về Ho_Chi_Minh

- Có cấu hình cập nhật thời gian theo giao thức NTP tới NTP Server

Vào phần **System Administration > Time Settings** > click vào **Edit Settings...**

Tích vào phần **Use Network Time Protocol** điền NTP server và Interface giao tiếp với NTP server



Ấn New để khai báo NTP server mới sau đó ấn OK

6. Khuyến cáo cấu hình SNMP

- Cấu hình đẩy SNMP tới hệ thống SNMP tập trung

SNMP của thiết bị không thể cấu hình trên giao diện web mà bắt buộc phải thực hiện cấu hình bằng cách gõ lệnh trực tiếp qua SSH

Thực hiện SSH vào thiết bị cấu hình tham khảo theo mẫu như sau

snmpconfig

Do you want to enable SNMP? [Y]> Y

Please choose an IP interface for SNMP requests.
1. Interface 1 (1.1.1.1/24)
2. Management (2.2.2.2/24)
[2]> 2

Enter the SNMPv3 passphrase.
> (Your SNMPv3 Passphrase)

Which port shall the SNMP daemon listen on?
[161]>161

Service SNMP V1/V2c requests? [N]> Y

Enter the SNMP V1/V2c community string.
[ironport]> (Your SNMP String)

From which networks shall SNMP V1/V2c requests be allowed? Separate multiple
networks with commas.
[2.2.2.2/24]>

Enter the Trap target as a host name, IP address or list of IP addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 2.2.2.10 (IP of Monitoring Server)

Enter the Trap Community string.
[ironport]> (Your SNMP String)

7. Yêu cầu về sử dụng mã hóa

- Có sử dụng tính năng SSL Inspection (nếu hệ thống hỗ trợ)

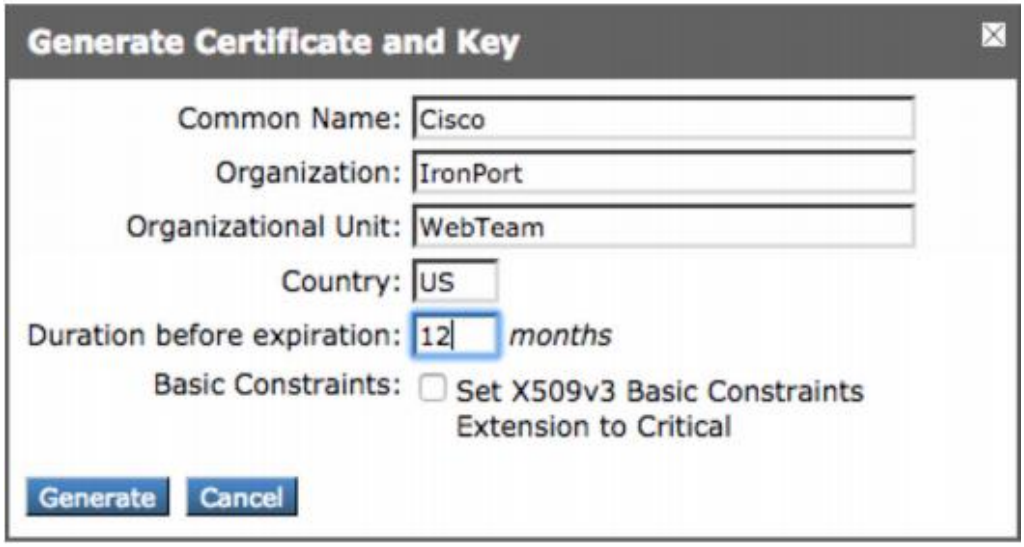
- Cấu hình trên proxy/web security gateway bypass không giải mã các trang web tin cậy về về tài chính ngân hàng, các web chứa thông tin cá nhân của người dùng như các trang mạng xã hội, email.

- Các bước thực hiện như sau

B1: ở phần **Security Services > HTTPS Proxy**. Click **Enable and Edit Settings**.

B2: Thực hiện tạo Certificate để chèn vào giữa giải mã các truy cập web sử dụng https lựa chọn **Use Generated Certificate and Key**.

B3: Click **Generated Certificate and Key** điền các thông tin tuỳ chọn và ấn **Generated**

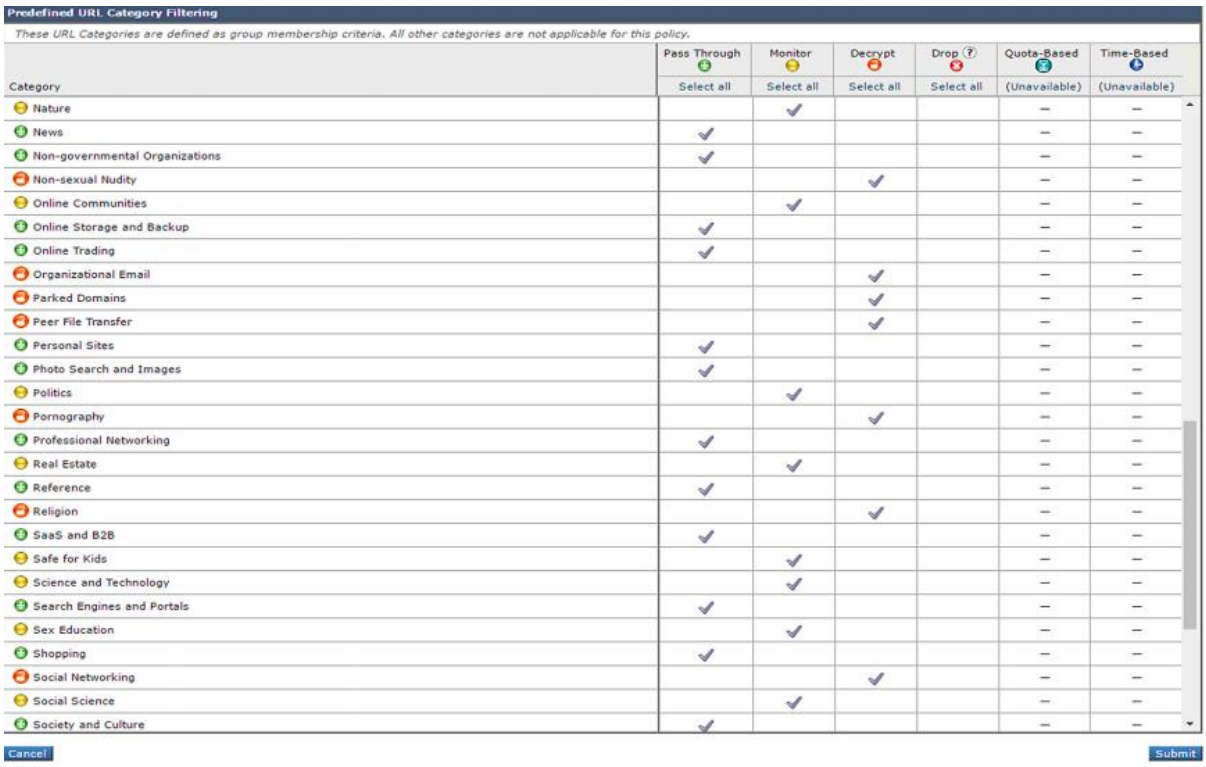


B4: Thực hiện **Submit** và **Commit** để save lại

B5: Download certificate về

B6: Tạo Policy để giải mã các traffic HTTPS bằng các truy cập vào **Web Security Manager > Decryption Policies**.

B7: Lựa chọn URL Categories muốn sẽ giải mã traffic HTTPS (Khuyến cáo không nên giải tích vào các category liên quan đến lĩnh vực tài chính ngân hàng hoặc lĩnh vực nhạy cảm chứa thông tin người dùng)



B8: Sau khi đã lựa chọn xong thực hiện **Submit** và **Commit**

8. Yêu cầu về ngăn chặn các C&C server điều khiển mã độc

- Thực hiện cập nhật thường xuyên danh sách C&C.

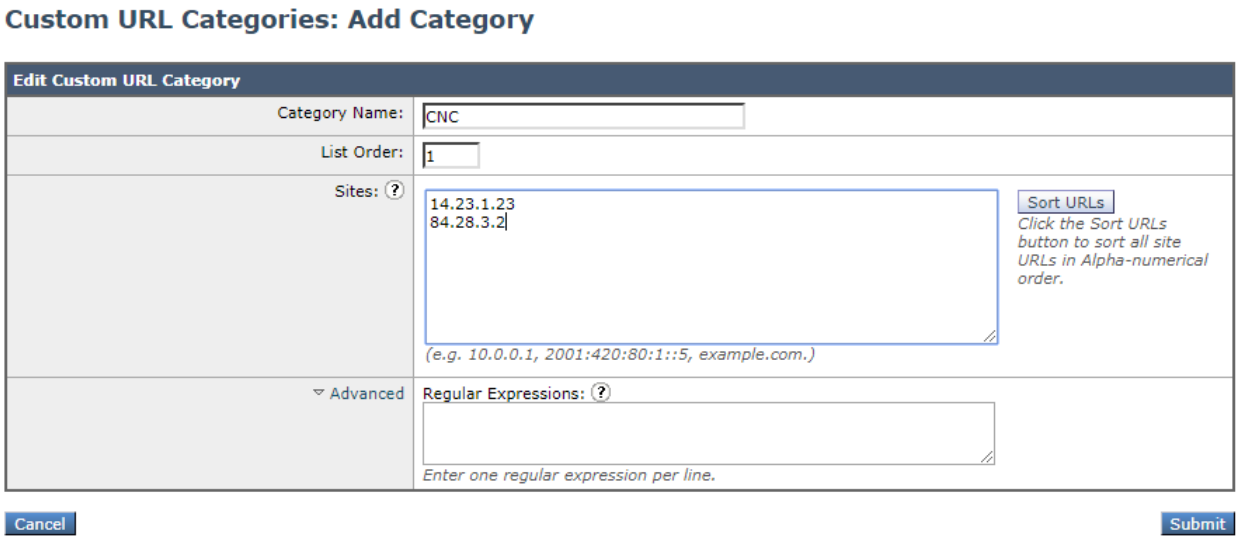
- Thực hiện chặn kết nối đến IP và domain của máy chủ điều khiển mã độc C&C theo các thông báo của bộ phận ATTT tại đơn vị

- Khuyến cáo nên thực hiện cài đặt policy theo hướng mặc định block all, chỉ mở những trang web nào cần mở

- Trong trường hợp ngược lại, hoặc muốn chặn cụ thể các trang web, server thực hiện các bước sau:

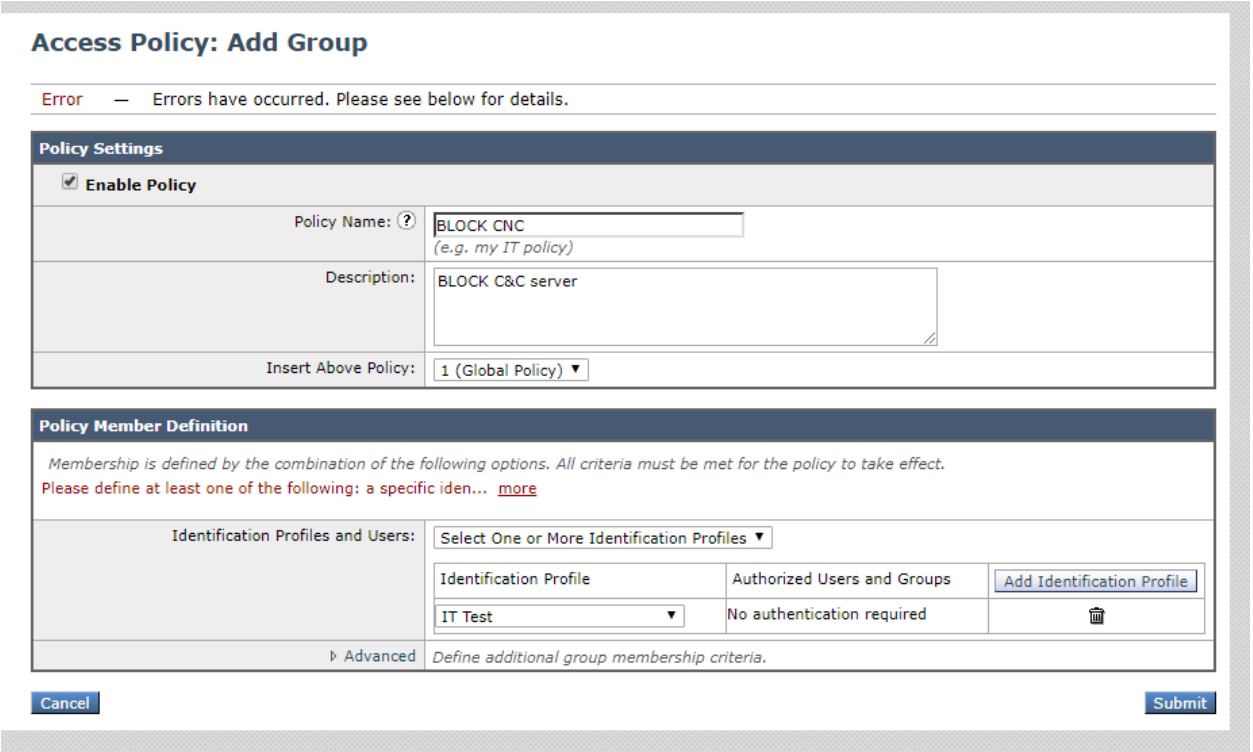
B1: Định nghĩa Category mới bằng cách vào **Web Security Manager** > **Custom URL Categories** > click vào **Add Custom Category**

B2: Tạo tên cho Custom Category và điền các IP hoặc URL muốn block sau đó ấn **Submit**

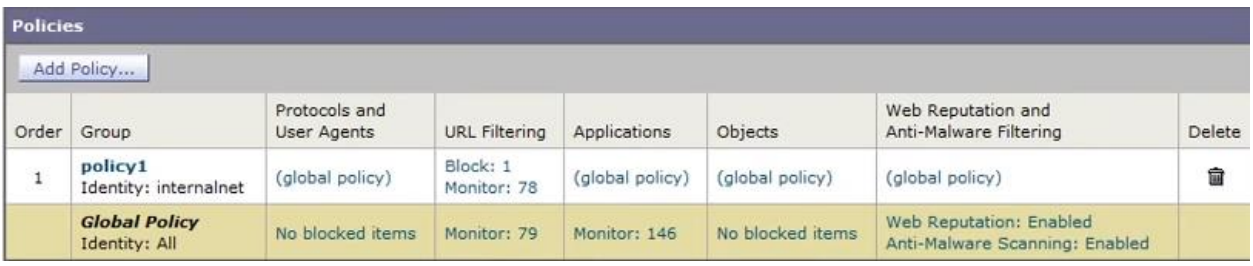


B3: Thực hiện vào **Web Security Manager** > **Access Policies** > Ấn vào **Add Policy** hoặc chọn policy cần điều chỉnh.

B4: Đặt tên cho Policy và gán Profiles hoặc nhóm Users sẽ dùng sau đó Submit

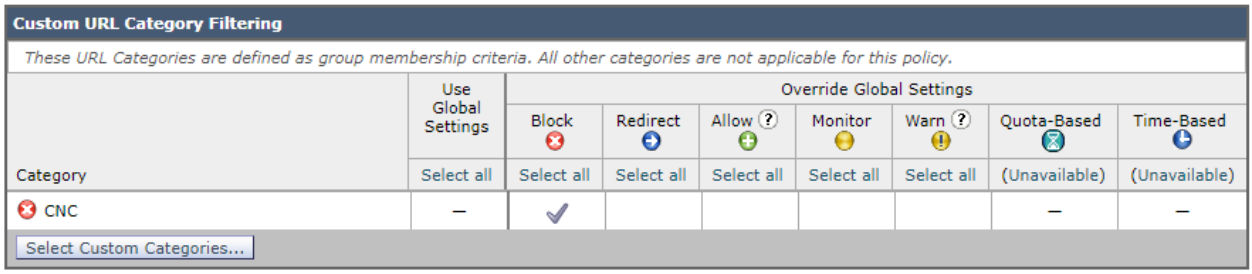


B5: Thực hiện Click vào phần URL Filtering của Policy muốn thay đổi



B6: Click vào phần Select Custom Categories Category nào muốn thêm vào thì chọn Include in policy và ấn apply

B7: Thực hiện các tùy chọn như Block hoặc Allow cho Category mới tạo và **Submit**



9. Yêu cầu về kiểm soát ứng dụng

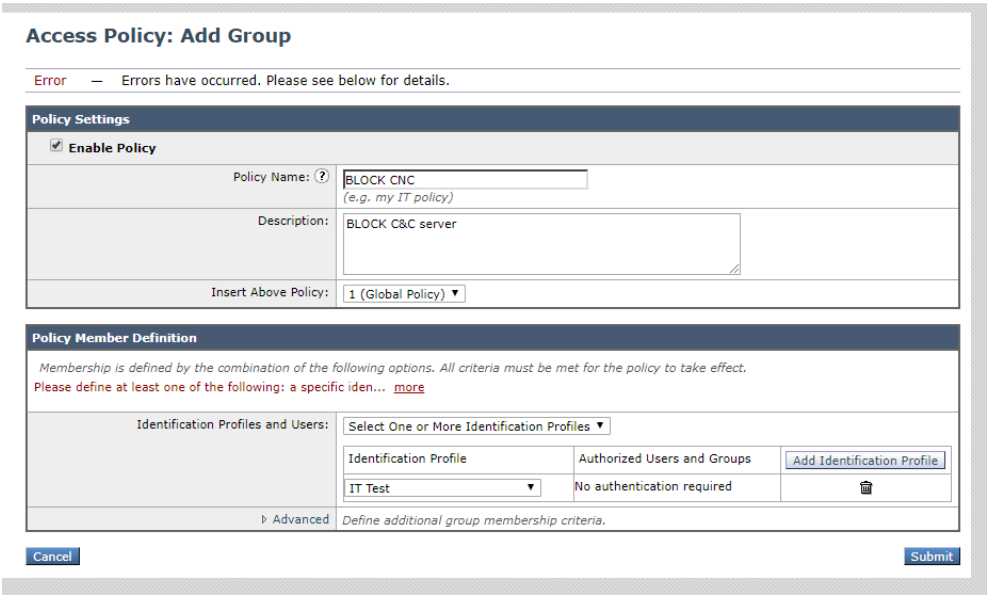
- Có bật tính năng kiểm soát kết nối đến ứng dụng (nếu có hỗ trợ)

- Thực hiện chặn kết nối đến các máy chủ điều khiển từ xa (như Teamviewer, Logmein, Ultraviewer)

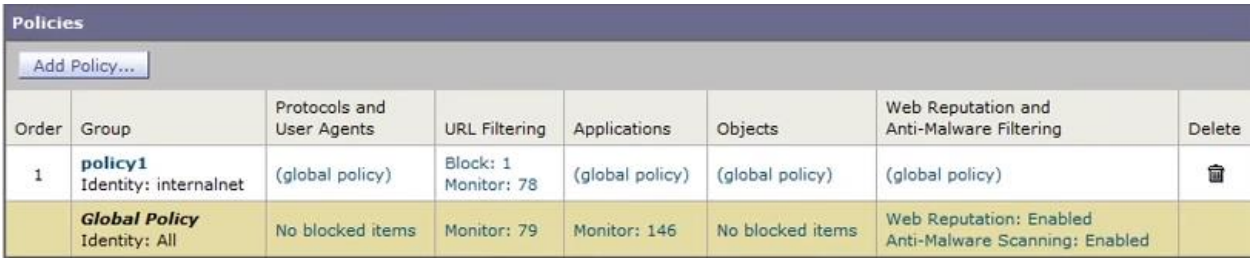
Cách thực hiện như sau

B1: Thực hiện vào **Web Security Manager** > **Access Policies** > Ấn vào **Add Policy** hoặc chọn policy cần điều chỉnh.

B2: Đặt tên cho Policy và gán Profiles hoặc nhóm Users sẽ dùng sau đó Submit



B3: Thực hiện Click vào phần Applictions của Policy muốn thay đổi



B4: Ở phần Presentation/conferencing lựa chọn application muốn block và submit

10. Yêu cầu về chặn lọc các website (URL Filtering)

- Có định nghĩa các loại trang web, các trang web độc hại, không phù hợp không được truy cập tới.

- Có định nghĩa các loại trang web, các trang web có tính chất không phù hợp với công việc, không được truy cập hoặc giới hạn truy cập trong giờ làm việc hành chính.

- Có cập nhật các loại trang web, danh sách trang web thường xuyên bao gồm các loại trang web được phép và không được phép truy cập tới.

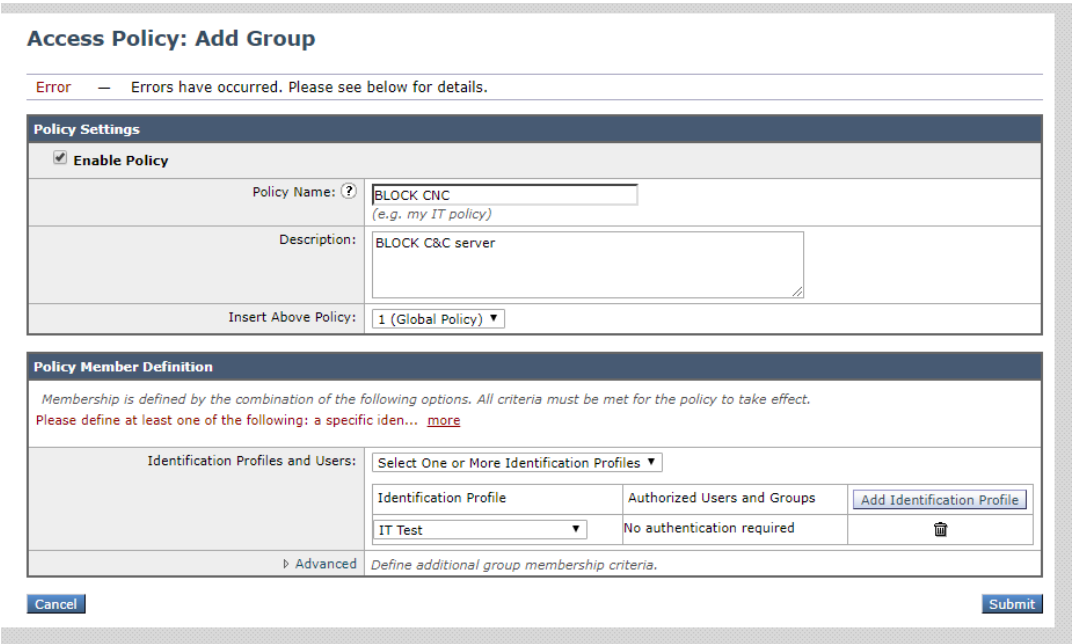
- Cấu hình chỉ được kết nối đến các trang web được phép truy cập.

- Cấu hình chặn không cho kết nối tới các trang web không được phép truy cập

Muốn chặn hoặc mở cụ thể các trang web, server thực hiện các bước sau:

B1: Thực hiện vào **Web Security Manager > Access Policies >** Ấn vào **Add Policy** hoặc chọn policy cần điều chỉnh.

B2: Đặt tên cho Policy và gán Profiles hoặc nhóm Users sẽ dùng sau đó Submit



B3: Thực hiện Click vào phần URL Filtering của Policy muốn thay đổi

Policies

Add Policy...

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Web Reputation and Anti-Malware Filtering	Delete
1	**policy1** Identity: internalnet	(global policy)	Block: 1 Monitor: 78	(global policy)	(global policy)	(global policy)	
	Global Policy Identity: All	No blocked items	Monitor: 79	Monitor: 146	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	

B4: Tích vào block các Category và Web muốn chặn

Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

Select Custom Categories...

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Block Select all	Monitor Select all	Warn Select all	Quota-Based (Unavailable)	Time-Based (Unavailable)
Real Estate		✓		–	–
Reference		✓		–	–
Religion		✓		–	–
SaaS and B2B		✓		–	–
Safe for Kids		✓		–	–
Science and Technology		✓		–	–
Search Engines and Portals		✓		–	–
Sex Education		✓		–	–
Shopping		✓		–	–
Social Networking	✓			–	–
Social Science		✓		–	–
Society and Culture		✓		–	–
Software Updates		✓		–	–
Sports and Recreation		✓		–	–
Streaming Audio		✓		–	–

11. Yêu cầu về chặn lọc Virus

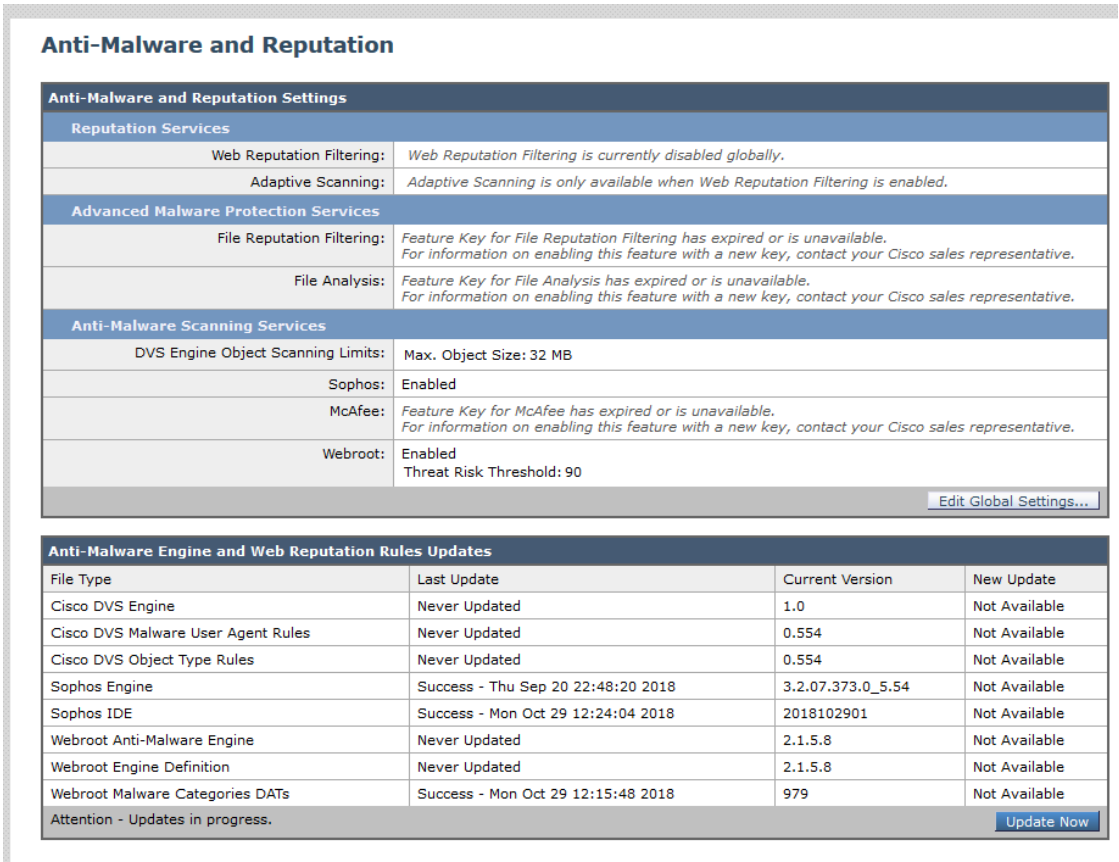
- Các yêu cầu này thực hiện dành cho các thiết bị có tích hợp và hỗ trợ tính năng AntiVirus

- Cập nhật thường xuyên các mẫu virus mới nhất.

- Có bật tính năng quét virus, phát hiện file độc hại được tải xuống từ website.

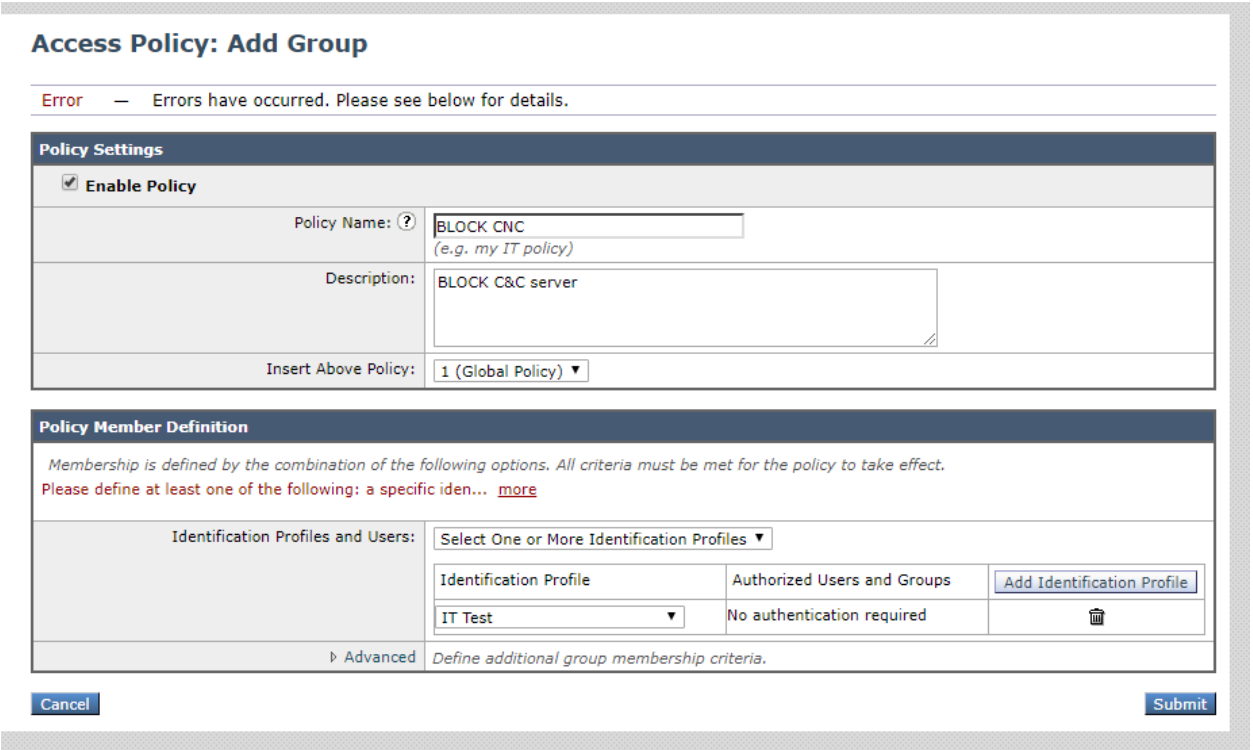
B1:Vào phần Security Services > Anti-Malware and Reputation

Đảm bảo thiết bị có license anti virus và được cập nhật mới nhất

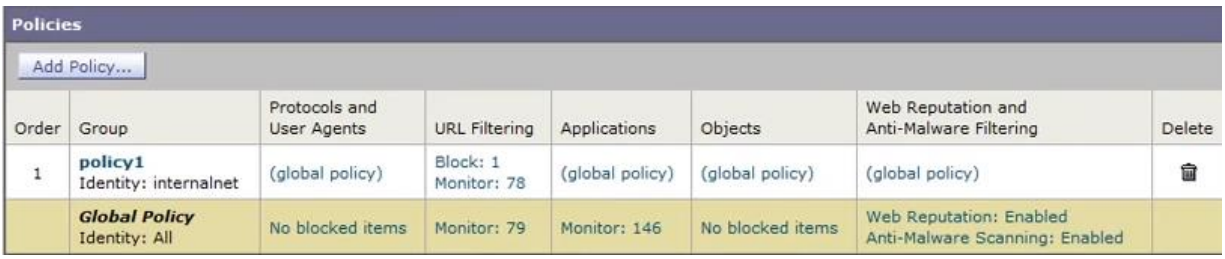


B2: Thực hiện vào **Web Security Manager** > **Access Policies** > Ấn vào **Add Policy** hoặc chọn policy cần điều chỉnh.

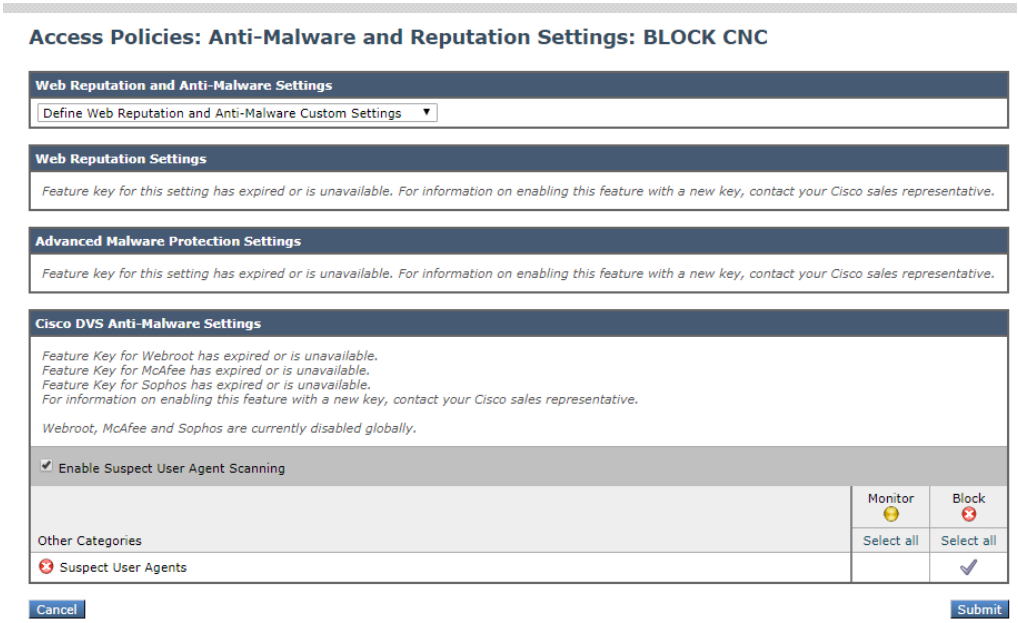
B3: Đặt tên cho Policy và gán Profiles hoặc nhóm Users sẽ dùng sau đó Submit



B4: Thực hiện Click vào phần Anti-Malware and Reputation của Policy muốn thay đổi



B5: Ở phần **Web Reputation and Anti-Malware Settings** thực hiện chọn như bên dưới > Tích vào **Enable Suspect User Agent Scanning > Chọn action Block hoặc monitor và submit**



12. Yêu cầu chặn file upload

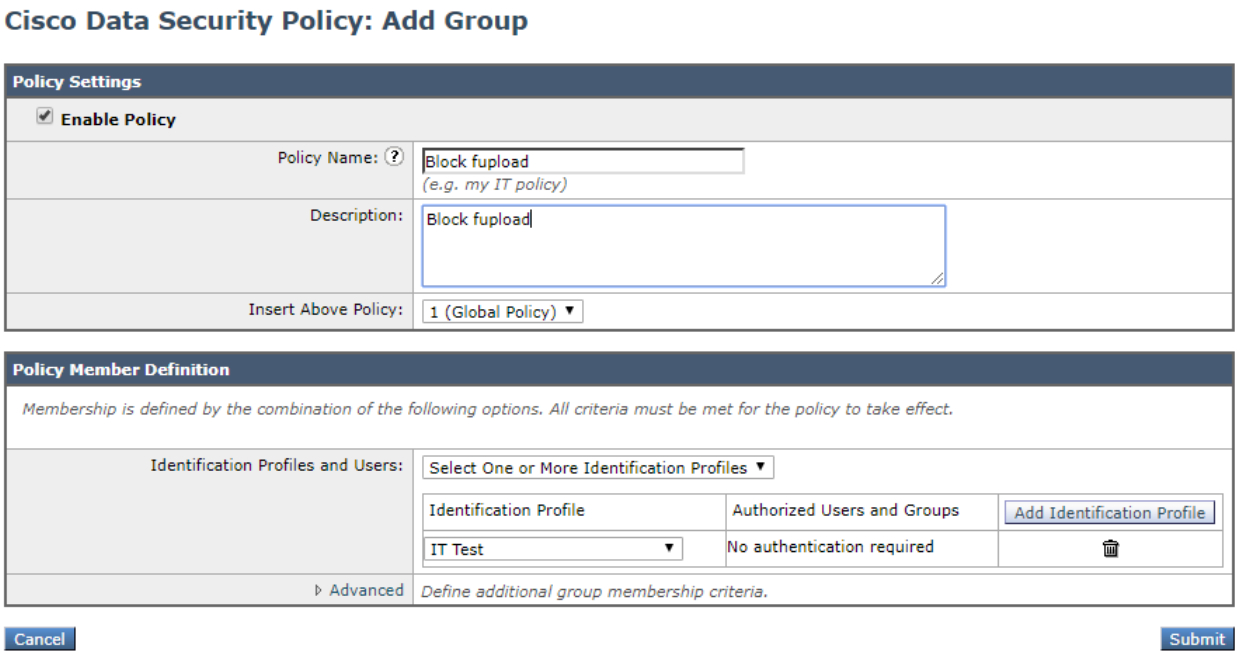
- Thực hiện chặn người dùng upload tài liệu lên các trang chia sẻ dữ liệu trực tuyến, truy cập public email, mạng xã hội

Ví dụ thực hiện chặn upload lên Google Drive thực hiện như sau, các trang khác làm tương tự

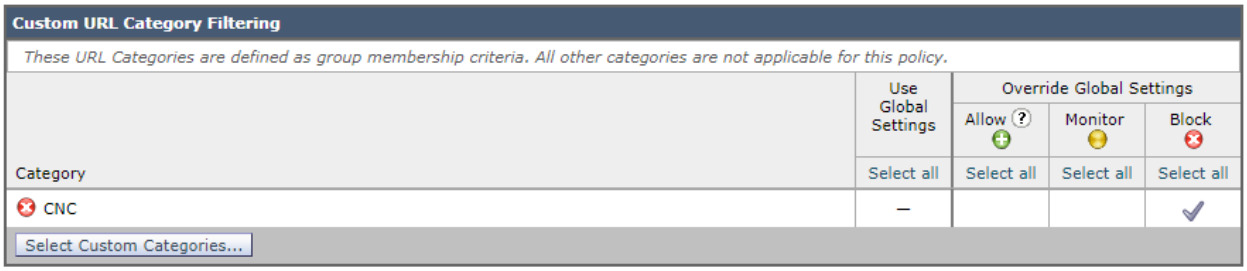
B1: vào phần **Security Services > Cisco Data Security Filters > Edit Settings**

Đảm bảo Cisco Data Security Filters Status đã được Enables

B2: Vào phần **Web Security Manager > Cisco Data Security>** Tạo mới Policy bằng cách Add Policy > đặt tên và lựa chọn Group user sẽ áp Policy



B3: Ở phần Policy click vào phần **URL Filtering** để lựa chọn các web site/category muốn chặn upload file



B4: Tích vào phần category muốn block upload file và **submit**

13. Yêu cầu về lưu log hệ thống

- Lưu đầy đủ log truy cập của người dùng, thông tin log bao gồm địa chỉ IP nguồn, IP đích, tên user, thời gian, URL truy cập, method, mã trả về, content type trả về, User Agent, Referer.

- Vào phần **System Administration > Log Subscriptions>** click **Add Log Subscription**

- Cấu hình các tham số như sau:

+ **Log Type:** Lựa chọn loại log sẽ đẩy, khuyến cáo lựa chọn nhiều loại log, tối thiểu phải có các loại sau:

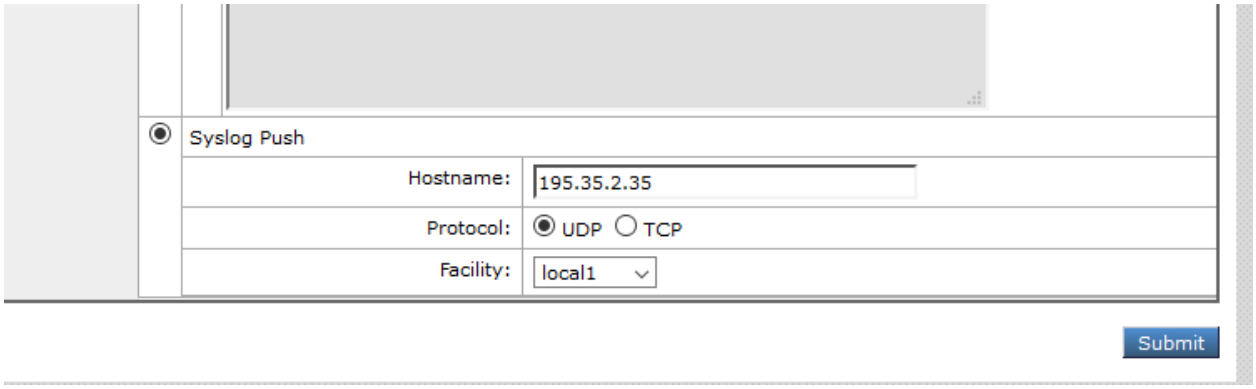
- Access Logs
- Audit Logs
- Proxy Bypass Logs
- GUI Logs
- CLI Audit Logs
- Configuration Logs

- Logging Logs
- Data Security Logs
- Default Proxy Logs
- McAfee Logs (Nếu có mua license check virus của McAfee)
- System Logs
- Traffic Monitor Error Logs
- Traffic Monitor Logs
- Updater Logs
- Upgrade Logs
- Web Categorization Logs
- Reporting Query Logs
- OCSP Log

+ **Log Name:** Điền tên tùy chọn
+ **File Name:** Để mặc định hoặc đặt tên riêng
+ **Maximum File Size:** Sử dụng cấu hình Default

Tích vào phần Syslog Push điền thông tin IP server lưu log, protocol và Facility

Sau đó submit



- Tất cả log được lưu tối thiểu 3 tháng để rà soát trong trường hợp cần thiết.

Phụ lục 12.
HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HỆ THỐNG KASPERSKY SECURITY CENTER

1. Yêu cầu về việc cài đặt Hệ thống antivirus tập trung an toàn

- Các thành phần của hệ thống Antivirus tập trung phải được cài đặt trên hệ điều hành an toàn, đã được thiết lập cấu hình chính sách bảo mật đảm bảo Quy tắc cấu hình ATTT cho hệ điều hành.

- Phiên bản cài đặt phải là phiên bản vẫn duy trì các bản vá cập nhật bởi nhà sản xuất, được cập nhật bản vá và đảm bảo không mắc các lỗ hổng bảo mật đã được công bố.

- Không sử dụng các account thuộc nhóm Domain Admins, Schema Admins hoặc Enterprise Admin cài đặt.

2. Yêu cầu môi trường vận hành an toàn

- User remote quản trị hệ thống Antivirus phải enable cơ chế xác thực đa nhân tố (token/OTP).

- Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho máy người dùng cuối để vận hành các hệ thống antivirus.

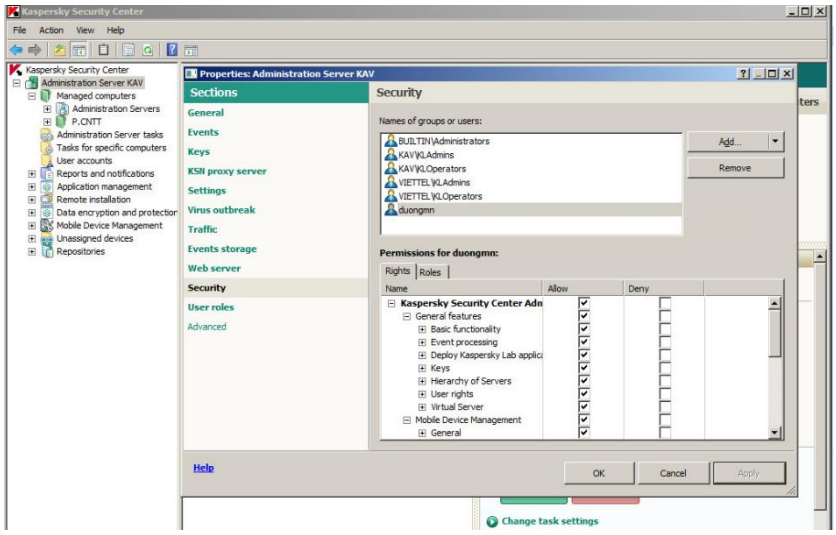
- Các máy riêng không dùng để sử dụng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MS Office/pdf) chỉ sử dụng để vận hành hệ thống.

3. Yêu cầu về thiết lập chính sách trên hệ thống antivirus tập trung

3.1. Phân quyền cho user quản trị từ xa (remote console)

- Đối với quản trị viên toàn bộ hệ thống Antivirus tập trung

+ Dùng tool Kaspersky Security Center – chọn Server – Chuột phải – Properties – Add tài khoản quản trị toàn bộ hệ thống vào và click Full quyền cho User này trong mục Rights.

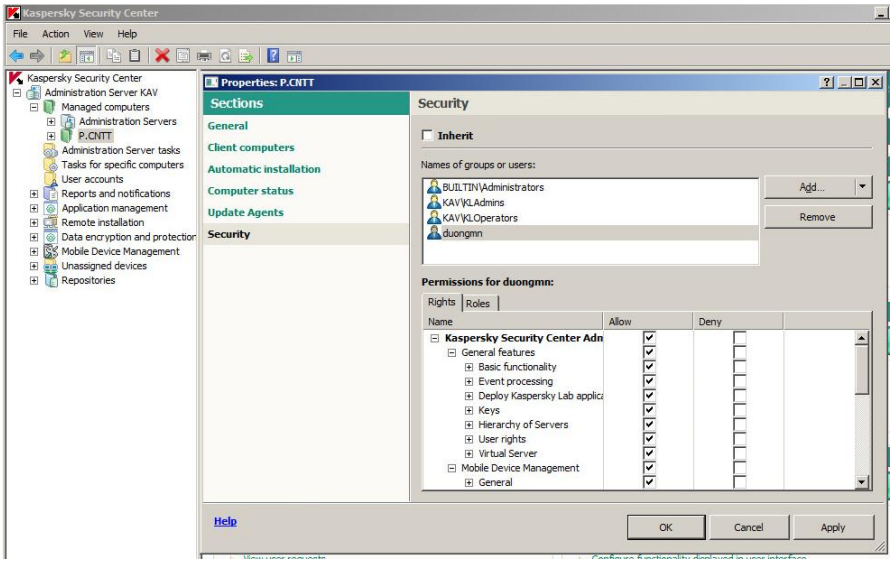


- Đối với quản trị viên 1 Group trong hệ thống Antivirus tập trung

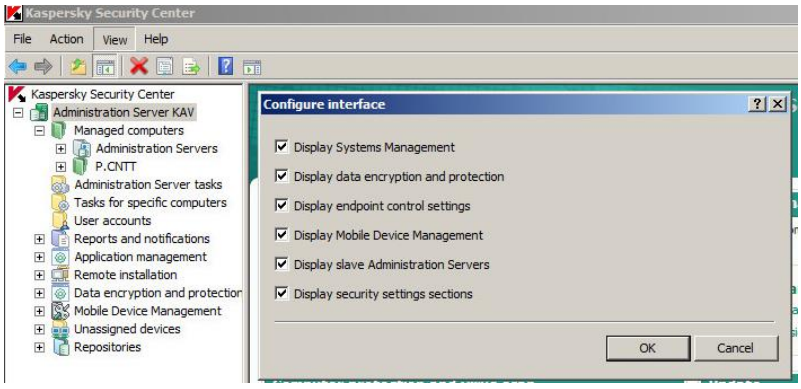
+ Dùng tool Kaspersky Security Center – chọn Server – Chuột phải – Properties – Add tài khoản quản trị 1 Group vào và chọn những quyền sau:

- Kaspersky Security Center Admin – General features – Basic functionality: Read
- Kaspersky Security Center Admin – General features – Deploy Kaspersky Lab applications – Read, Modify, Execute, Manage Kaspersky Lab patches
- Kaspersky Security Center Admin – System Management – Remote installation – Read, Modify, Execute

- Sau đó nếu muốn phân quyền cho 1 user được phép quản trị 1 nhóm bất kỳ, thì sử dụng công cụ Kaspersky Security Center – Managed computers – chọn Group cần phân quyền – Properties – Security, bỏ chọn Inherit, add thêm user cần phân quyền, và trong mục Rights click các quyền cần thiết.



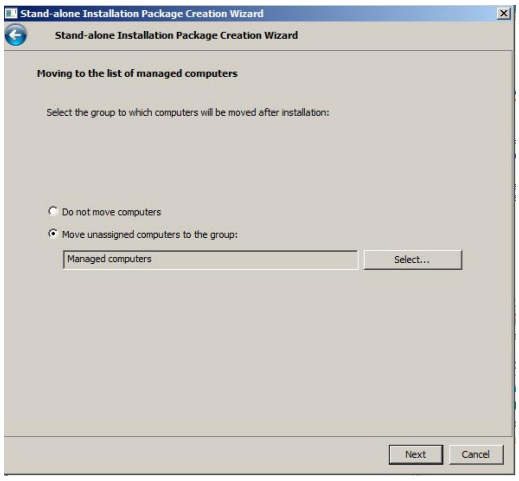
- Trong trường hợp không có tab Security thì sử dụng công cụ Kaspersky Security Center chọn vào Server – View – Configure interface – click toàn bộ các option có thể.



3.2. Cài đặt tự động Net Agent và Kaspersky endpoint security

- Cài đặt tự động Net Agent cho các máy join AD

+ Trên Kaspersky Security Center tạo 1 gói stand-alone chỉ bao gồm Network agent nếu chưa có: Vào Remote Installation – Installation packages – Chọn Kaspersky Security Center Network Agent và click vào Create stand-alone installation package. Trong bước tiếp theo chọn Move unassigned computers to groups vào Group computer, mặc định là "Managed computers". Các bước tiếp theo chọn mặc định



+ Sau khi tạo được gói cài đặt stand-alone thì sẽ có đường dẫn đến file này, ví dụ: "\\192.168.30.34\klshare\PkgInst\NetAgent_10.2.434\setup.exe", có thể sửa lại tên file, thư mục hoặc chuyển sang 1 thư mục chia sẻ khác mà máy tính người dùng có thể kết nối đến được.

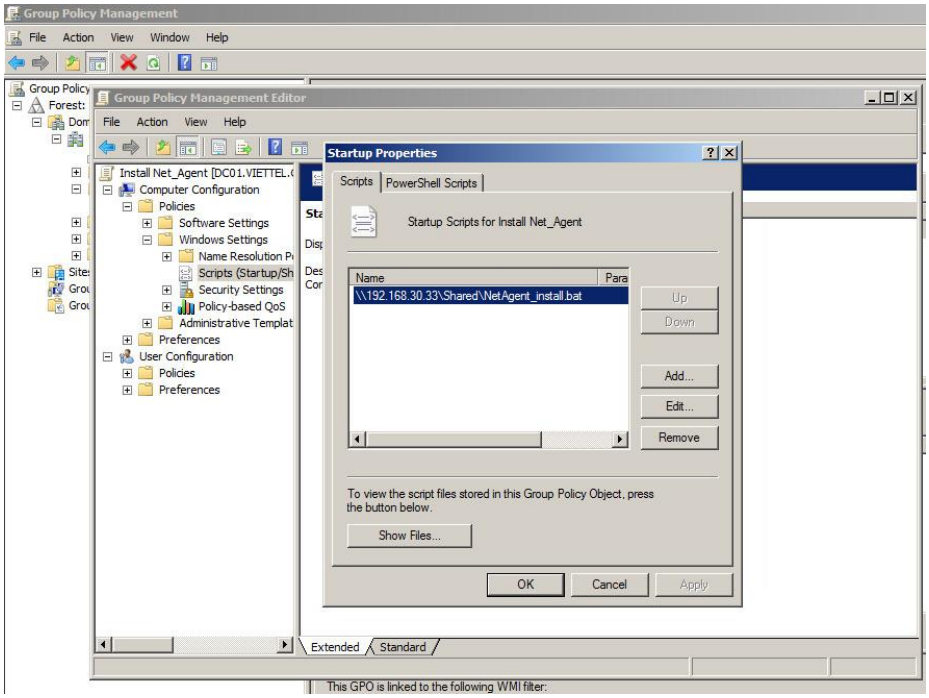
+ Tạo 1 script .bat với nội dung sau để cài đặt cho các máy join Active Directory mà chưa cài đặt Net Agent. Nếu đã cài Net Agent rồi thì chỉnh lại server cho chính xác (Trong trường hợp cài Net Agent từ đơn vị khác chuyển sang)

```
@echo off

if exist "C:\Program Files\Kaspersky Lab\NetworkAgent\" (
	pushd "C:\Program Files\Kaspersky Lab\NetworkAgent"
	klmover.exe -address 192.168.30.34
	net start AVP
	sc config AVP start=auto
	net start klnagent
	sc config klnagent start=auto
	exit
) else if exist "C:\Program Files (x86)\Kaspersky Lab\NetworkAgent\" (
	pushd "C:\Program Files (x86)\Kaspersky Lab\NetworkAgent"
	klmover.exe -address 192.168.30.34
```

```
        net start AVP
        sc config AVP start=auto
        net start klnagent
        sc config klnagent start=auto
        exit
)

set
SHARE_PATH=\\192.168.30.34\klshare\PkgInst\NetAgent_10.2.4
34
set DEST_PATH="C:\KES_KCQ"

if exist %DEST_PATH% goto :caidat
        mkdir %DEST_PATH%%
        copy %SHARE_PATH%\setup.exe %DEST_PATH%
        %DEST_PATH%\setup.exe /s
        exit

:caidat
        copy %SHARE_PATH%\setup.exe %DEST_PATH%
        %DEST_PATH%\setup.exe /s

exit
```

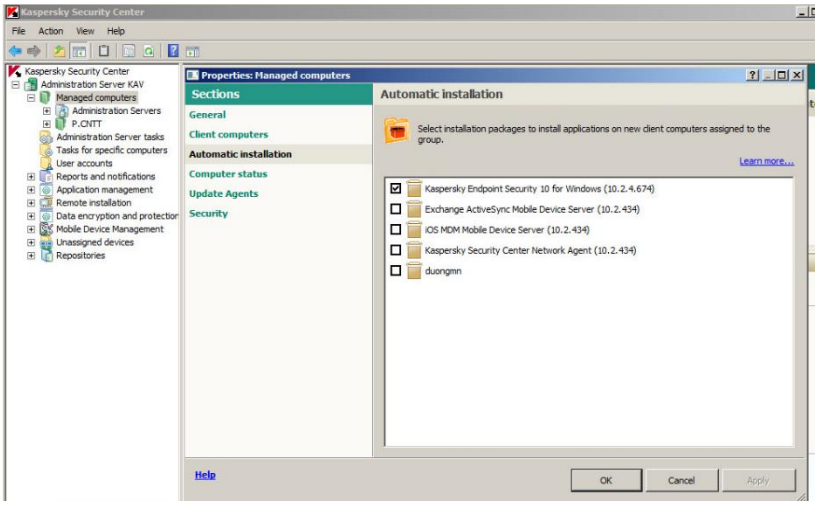
+ Lưu ý: Sửa lại địa chỉ IP của Kaspersky Security Center và đường dẫn download file cài đặt net Agent cho chính xác

+ Sau đó vào Active Directory tạo hoặc sửa GPO áp dụng cho các máy tính join vào AD, vào phần Computer Configuration – Policies – Windows Settings – Scripts – Startup. Mở tab Scripts và add Script phía trên vào. Lưu ý Script cũng phải ở thư mục share mà các máy tính trong AD có thể kết nối được

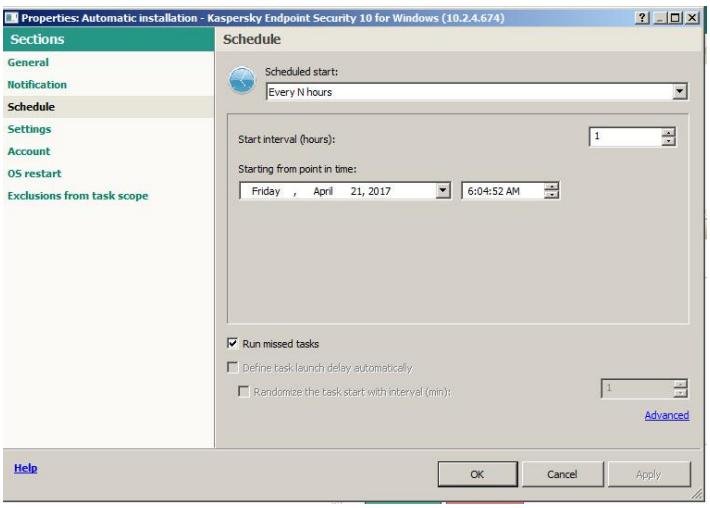


- Cài đặt tự động Kaspersky endpoint security (Chỉ áp dụng cho máy đã cài Network Agent)

+ Trong Kaspersky Security Center – vào Group computer muốn tự động cài đặt Kaspersky endpoint security (ví dụ trong thư mục Managed computers) – Properties – Automatic installation - Chọn Kaspersky Endpoint Security (lưu ý chọn phiên bản cho phù hợp) – click OK.



+ Sau khi thực hiện thì Kaspersky Security Center sẽ tự động tạo thêm Task là "Automatic installation – Kaspersky Endpoint Security 10 for Windows". Chọn Properties của task này – Schedule – chọn chạy 1 tiếng 1 lần và tích vào "Run missed tasks"



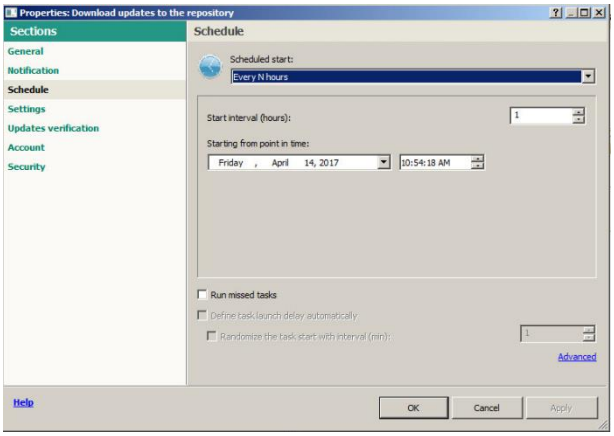
3.3. Thiết lập cấu hình cập nhật cho antivirus

- Cập nhật mẫu virus về máy chủ antivirus tập trung

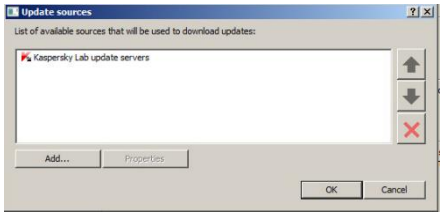
+ Vào phần Administration Server Tasks

+ Nếu đã có task với task type: Download updates to the repository rồi thì kiểm tra lại các tham số sau:

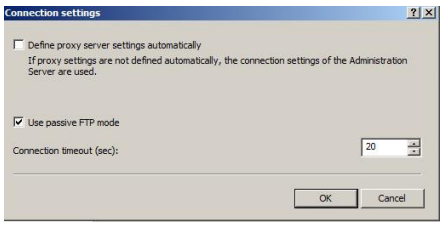
- Schedule: Tối thiểu phải 1 ngày 1 lần "chọn Every N days và chọn interval là 01 days. Recommend để 1 tiếng 1 lần (Mặc định).



- Settings:
- Phần Update Sources – Chọn Kaspersky Lab update servers (Mặc định).



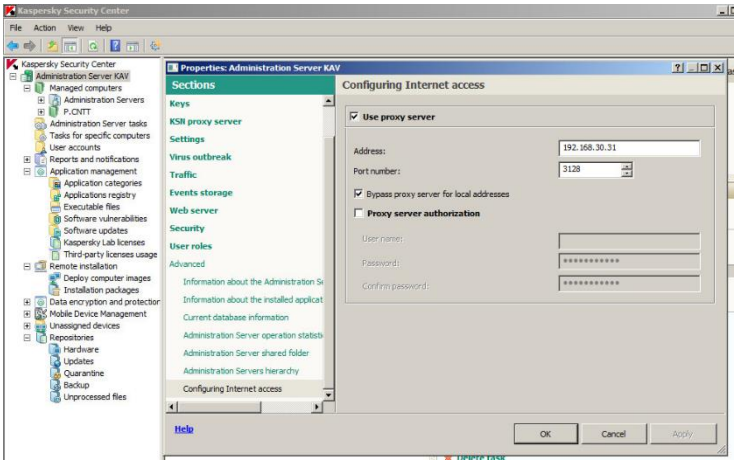
- Phần Connection Settings: Bỏ tích Define proxy .. và tích chọn Use passive FTP mode (Mặc định)



- Phần Updates list: Chọn Auto Detect Updates list (Mặc định)

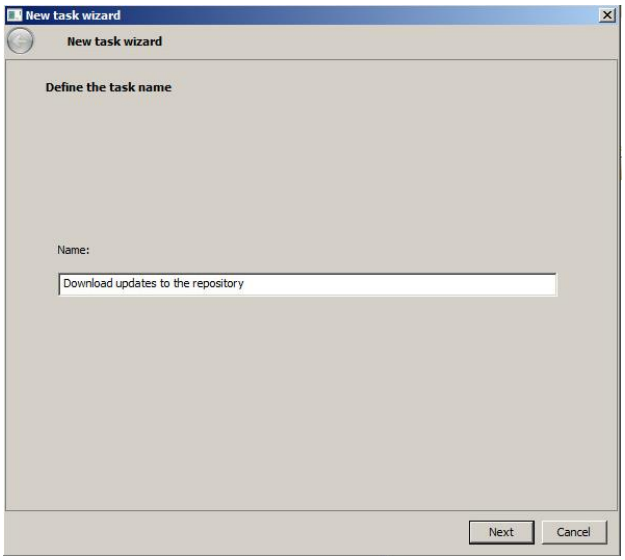
- Thiết lập update qua Proxy:

+ Trong Kaspersky Security Center – Chọn server Antivirus tập trung – Properties – Advance – Configure Internet access. Nhập địa chỉ IP và port của proxy, click Bypass proxy server for local address

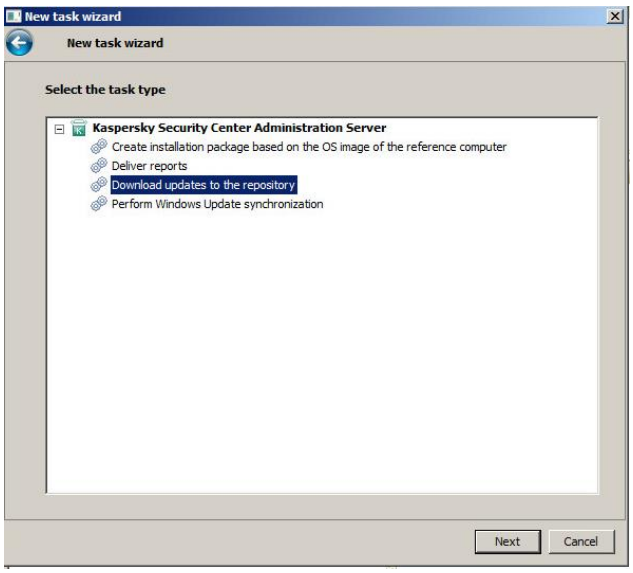


- Nếu chưa có task nào với task type: Download updates to the repository thì tạo 1 task mới

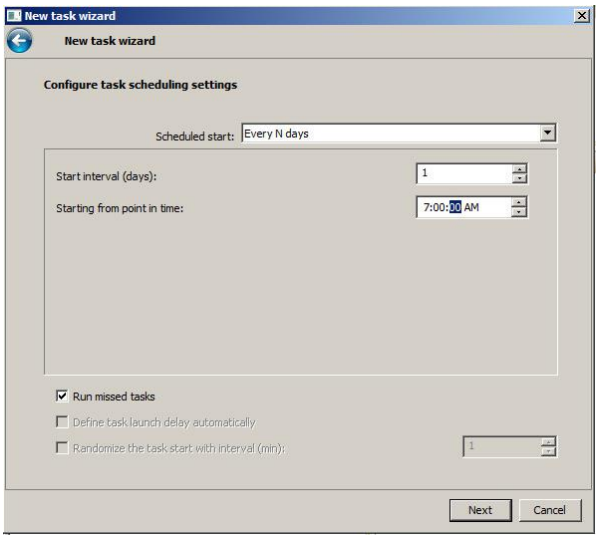
+ Create New task



+ Chọn Download updates to the repository. Lưu ý nếu đã có task update rồi thì sẽ không có lựa chọn này.



+ Tất cả các option để mặc định. Sau đó chỉnh sửa lại các option theo như mục " Nếu đã có task Download updates to the repository" phía trên.



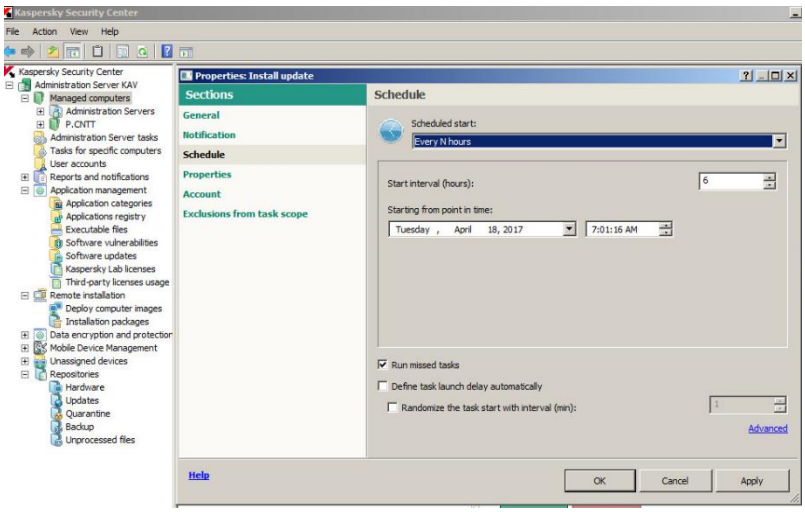
3.3. Cập nhật mẫu virus về antivirus client trên máy trạm

- Vào phần Managed Computers – Chọn Group muốn cấu hình – Task (Hoặc có thể cấu hình tại Managed Computers – Task để kế thừa cấu hình xuống các Group con)

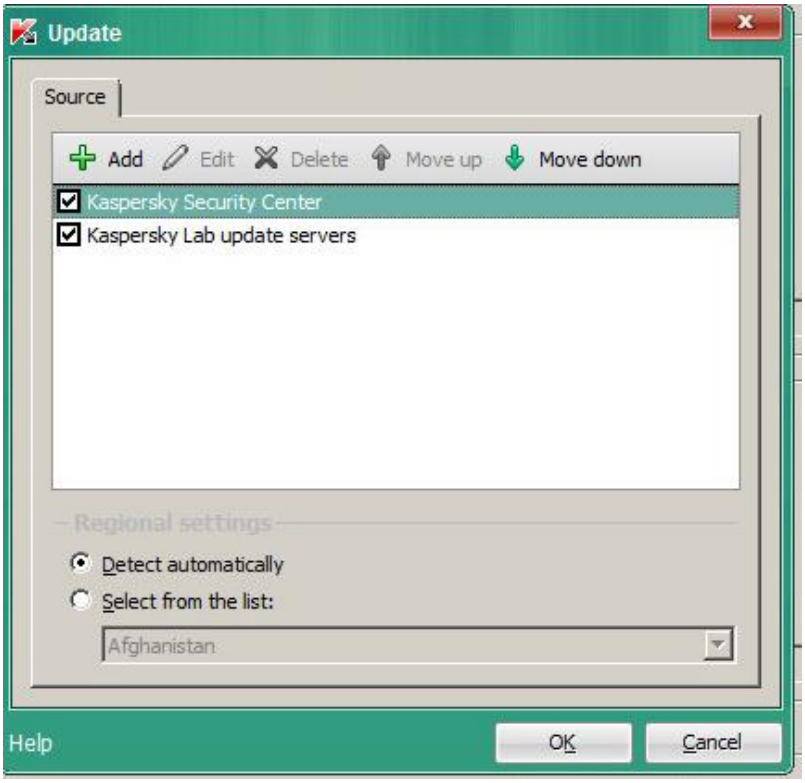
- Nếu đã có task với task type: Update rồi thì kiểm tra lại các tham số sau:

+ Phần Schedule để tối thiểu 1 ngày 1 lần.

+ Recommend: Every N hours và chọn interval 6h. Tích chọn Run missed tasks



+ Phần Properties – Application Update Settings – Update Source – Settings



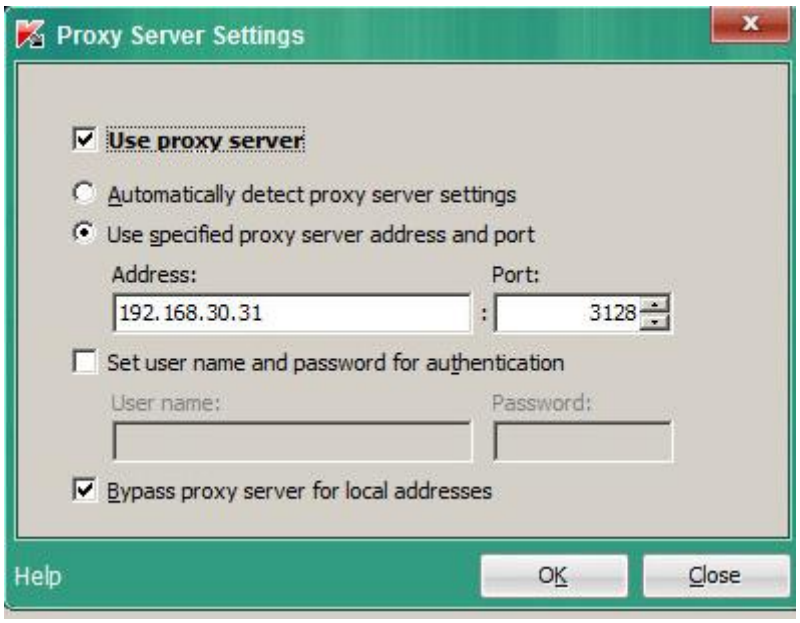
+ Click chọn:

  - Kaspersky Security Center: Update từ Antivirus server.
  - Kaspersky Lab update servers: Update từ Internet (thông qua proxy theo bước tiếp theo)

+ Chọn thứ tự ưu tiên trước sau tùy theo đơn vị.

- Tùy chọn update qua Proxy

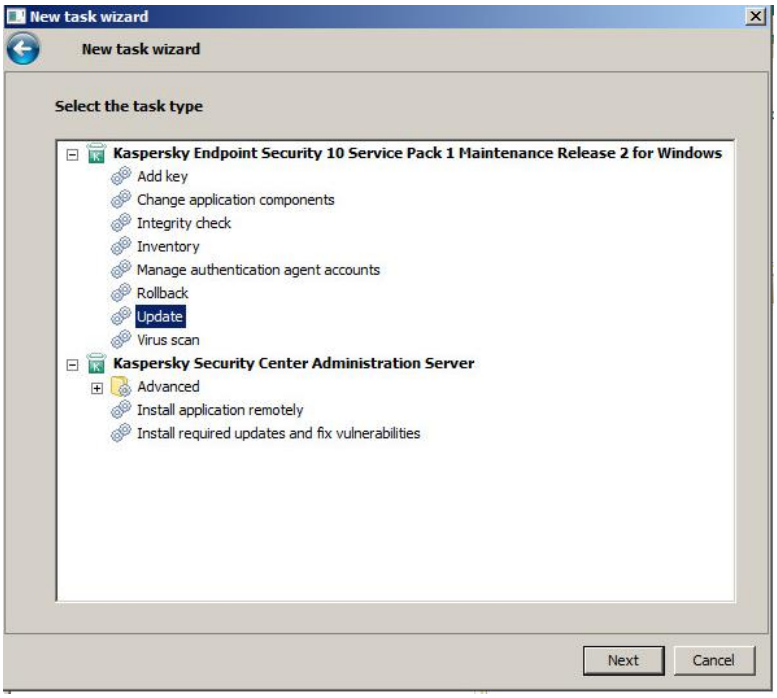
+ Vào phần Policy đang quản lý máy tính – Properties – Advanced Settings – Application Settings – Proxy Server Settings – Click Use Proxy server – Use specific proxy server address and port (Nhập địa chỉ IP proxy, port), click Bypass proxy server for local address.



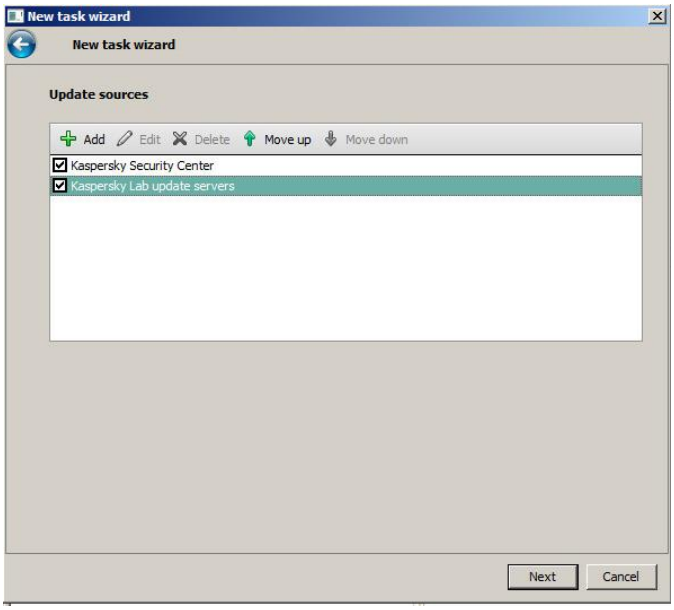
- Nếu chưa có task với task type: Update thì tạo 1 task mới

+ Chọn tạo 1 task mới

+ Task type chọn Update



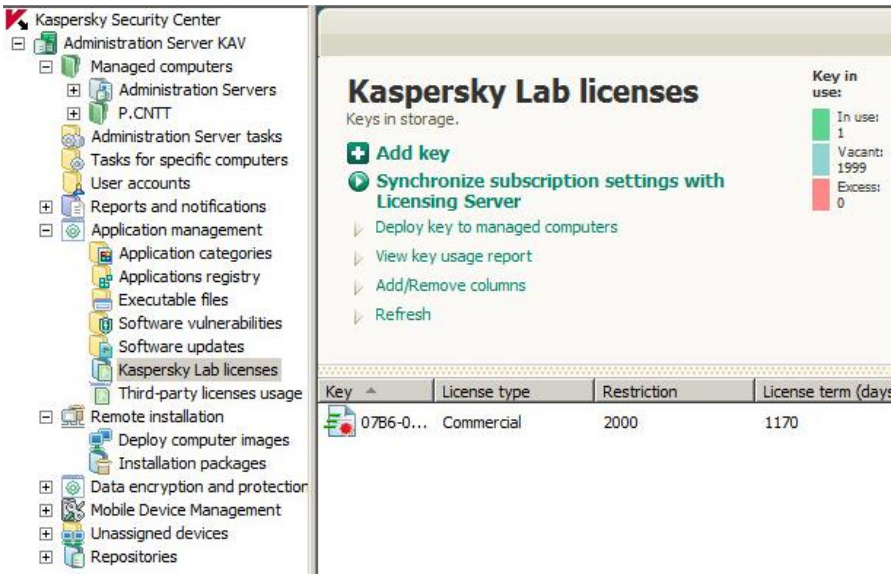
+ Update source chọn thêm Kaspersky Lab update server (Phần này có thể tùy chỉnh sau)



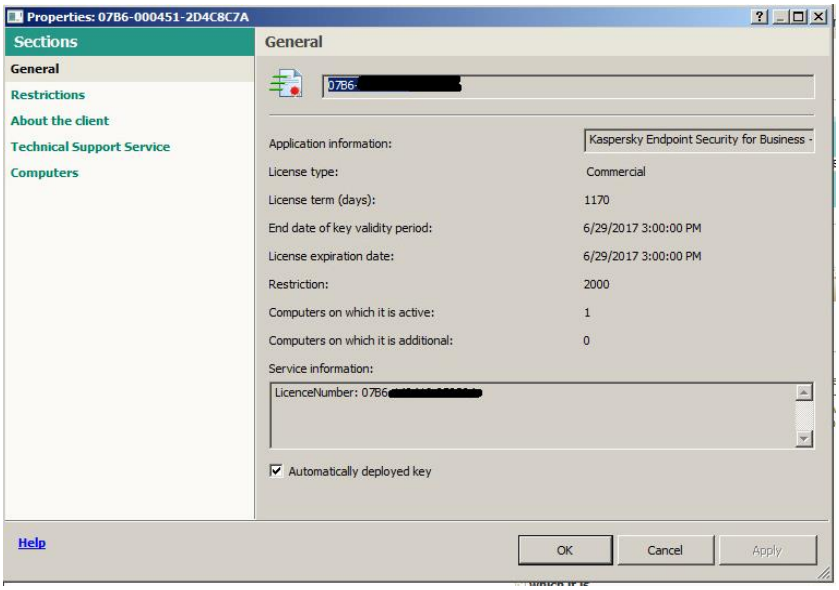
+ Các tùy chọn khác để mặc định. Sau khi tạo task xong tùy chỉnh lại task như mục "Nếu đã có task với task type: Update"

3.4. Quản lý license key tập trung

- Trong Kaspersky Security Center vào phần Application management – Kaspersky Lab License add các license đã có vào



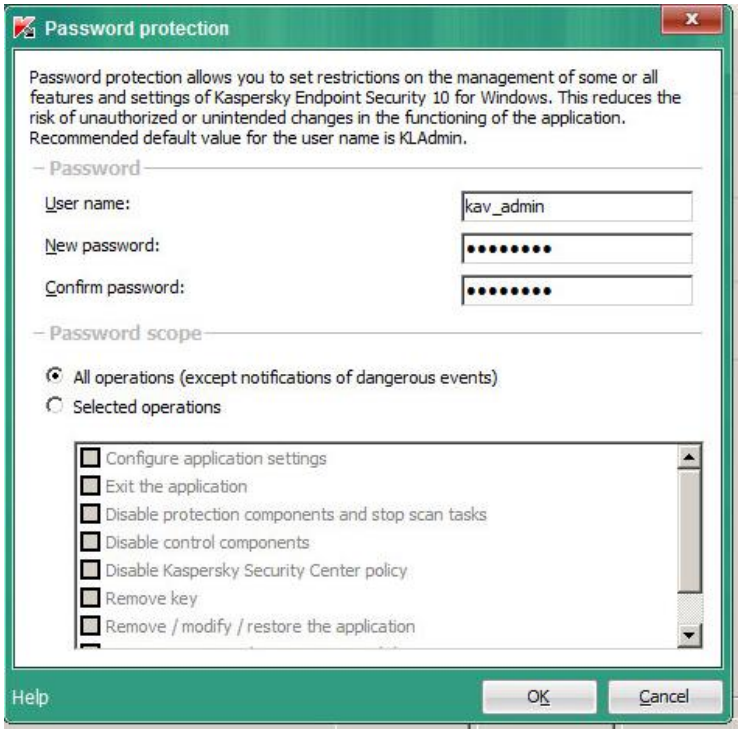
- Để license tự động active cho các máy cài đặt Kaspersky endpoint security thì chọn License – Properties – General – click vào Automatically deployed key



3.5. Không cho người dùng thay đổi tham số cấu hình và uninstall

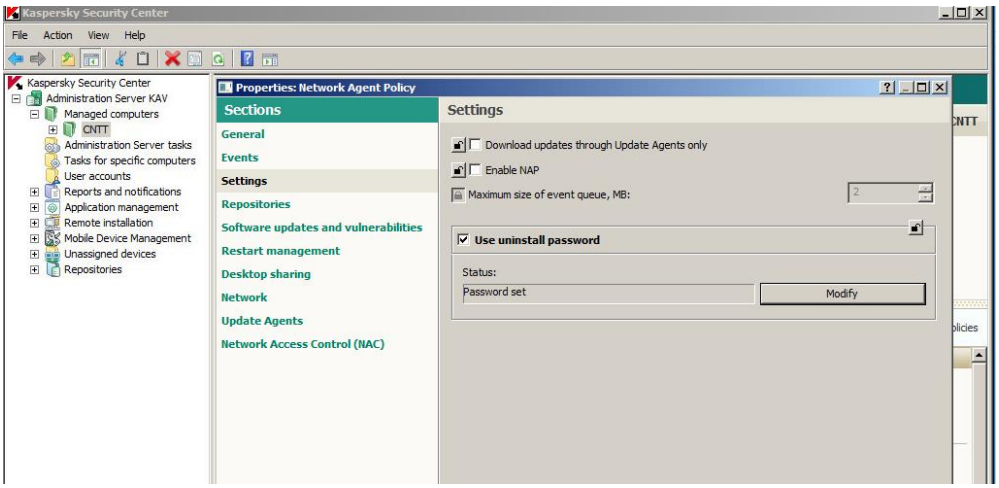
- Bảo vệ Kaspersky Endpoint Security không cho người dùng tùy chỉnh cấu hình và gỡ cài đặt:

+ Vào phần Policy đang quản lý máy tính – Properties – Advanced Settings - Interface - Tích vào Enable password protection – Settings: nhập username, password bảo vệ và chọn All operations



- Bảo vệ NetAgent không cho người dùng gỡ bỏ cài đặt

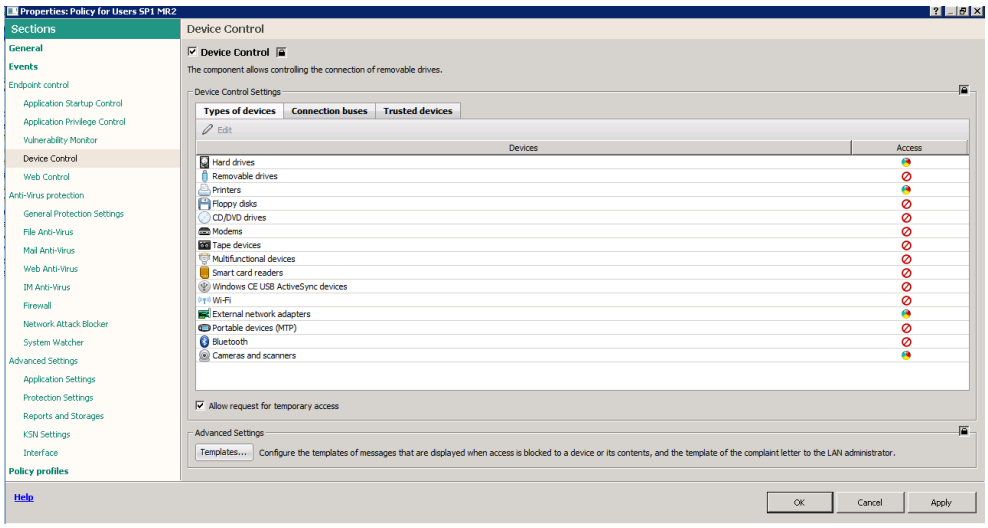
+ Chỉnh sửa Policy dành cho Network Agent (Nếu chưa có policy này thì tạo thêm) – Settings – Use uninstall password – Modify – Nhập password bảo vệ



3.6. Cấu hình chặn các thiết bị ngoại vi

- Vào phần Policy đang quản lý máy tính – Properties – Device Control - Tích vào Device Control – ở mục Types of devices chọn Block những loại device sau:

+ Removable drivers
+ Floppy disks
+ CD/DVD drivers
+ Modems
+ Tape devices
+ Multifunctional devices
+ Smart card readers
+ Windows CE USB ActiveSync devices
+ Wifi
+ Portable devices (MTP)
+ Bluetooth



3.7. Cấu hình tường lửa mềm trên máy người dùng

- Lưu ý:

+ Có thể quản lý tập trung firewall trên máy người dùng bằng 2 cách:

  - Quản lý Kaspersky Firewall bằng Kaspersky Security center
  - Quản lý Windows Firewall bằng Active Directory

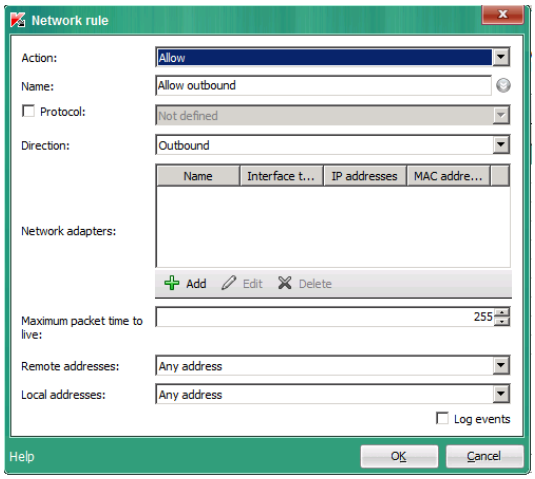
+ Chỉ dùng 1 trong 2 loại Windows Firewall hoặc Kaspersky Firewall. Nếu đã quản trị Kaspersky Firewall bằng Kaspersky Security center thì không quản trị Windows Firewall bằng Active Directory và ngược lại.

- Vào phần Policy đang quản lý máy tính – Properties – Firewall Tích vào Firewall và ở trong mục Firewall rules click vào Settings ở mục Configure rules for network packets and data stream:

- Ở cửa sổ mới mở ra, vào tab Network packet rules

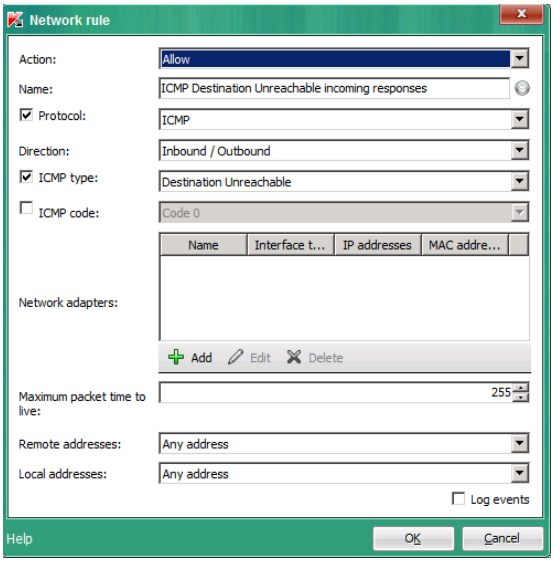
- Xóa hết toàn bộ những rule đang có, chỉ add thêm các rule sau:

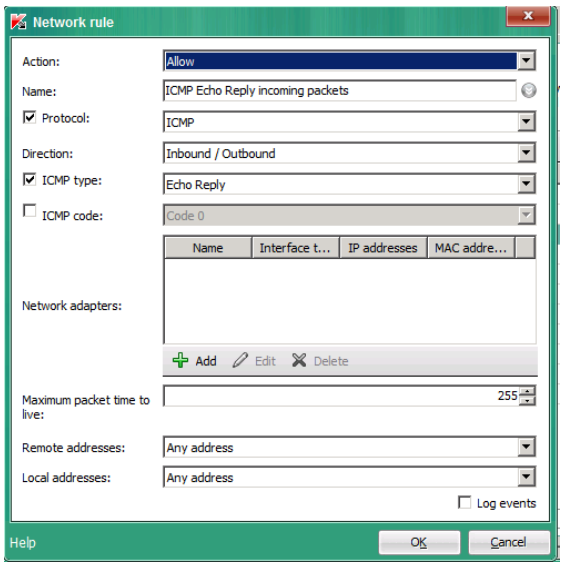
+ Rule 1: Allow outbound

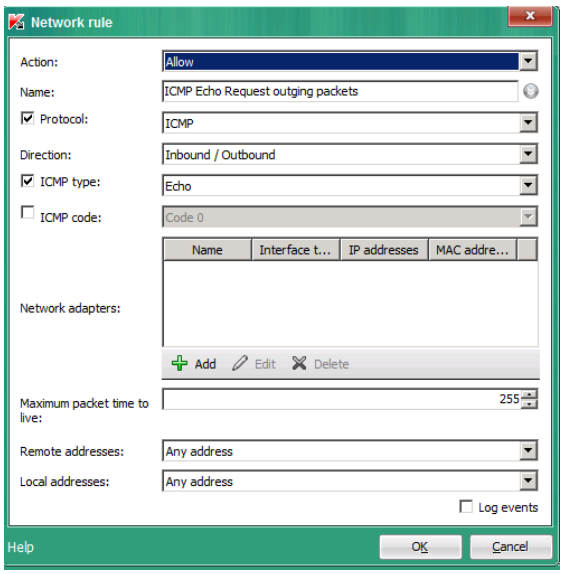


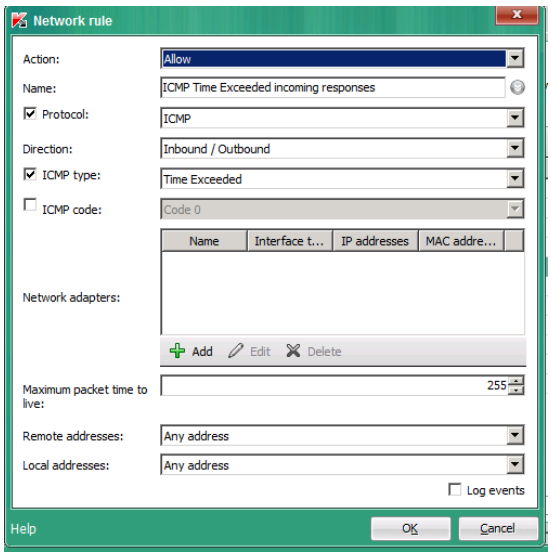
  - Chú ý phần Direction Outbound và Action: Allow

+ Rule 2 – 5 :

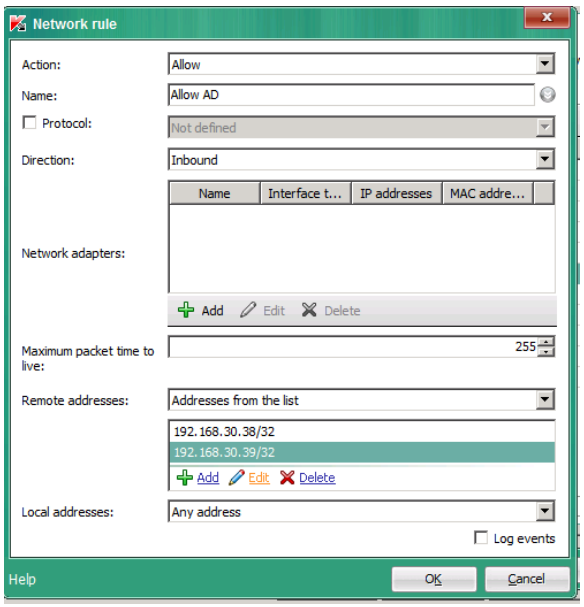






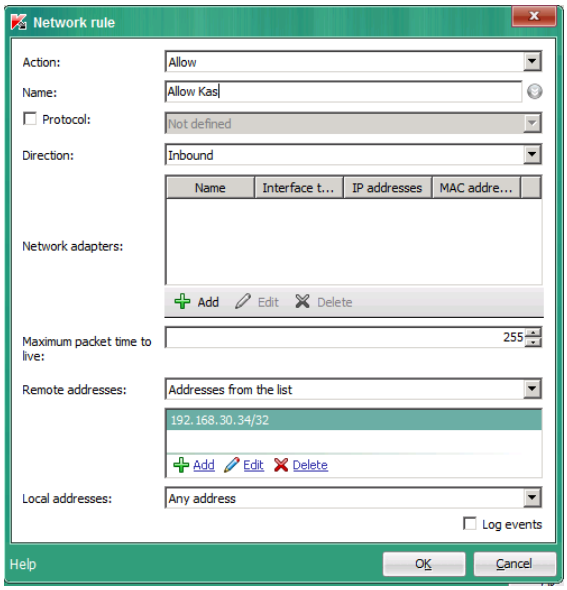


+ Rule 6: Cho phép kết nối từ AD



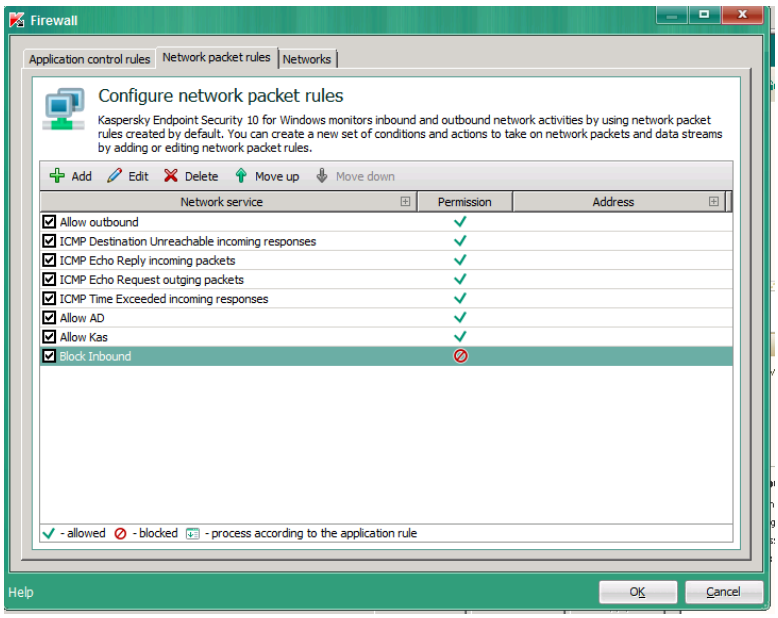
- Lưu ý: Trong phần Direction: Inbound, Action: Allow; Remote Address: add các địa chỉ của DC vào, Local address: any address.

+ Rule 7: Cho phép kết nối từ Kas



- Lưu ý: Trong phần Direction: Inbound, Action: Allow; Remote Address: add các địa chỉ của Kaspersky Security Center vào, Local address: any address.

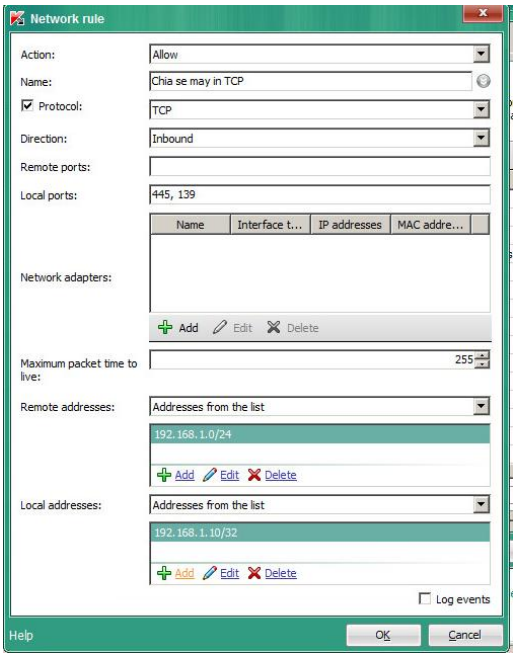
+ Rule cuối cùng: Block toàn bộ Inbound

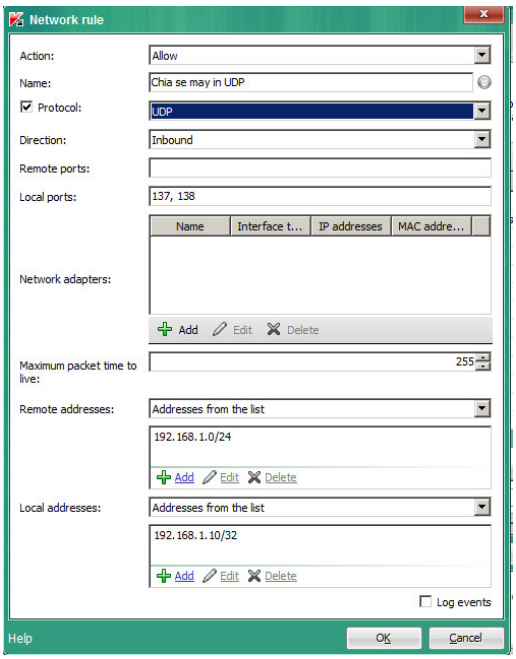


- Lưu ý: Đối với những trường hợp ngoại lệ cần mở kết nối vào máy tính người dùng cần tạo luật chỉ rõ cổng dịch vụ, địa chỉ nguồn, địa chỉ đích và các luật ngoại lệ này đặt trên luật Block Inbound cuối cùng, ví dụ:

+ Đối với các máy tính dùng để chia sẻ máy in: mở thêm chiều inbound port 445 (TCP), 139 (TCP), 137 (UDP), 138 (UDP). Lưu ý phải chỉ rõ địa chỉ nguồn (remote address), địa chỉ đích (local address). Ví dụ:

- Luật cho phép các máy tính trong dải 192.168.1.0/24 được truy cập máy in share từ máy 192.168.1.10/32.



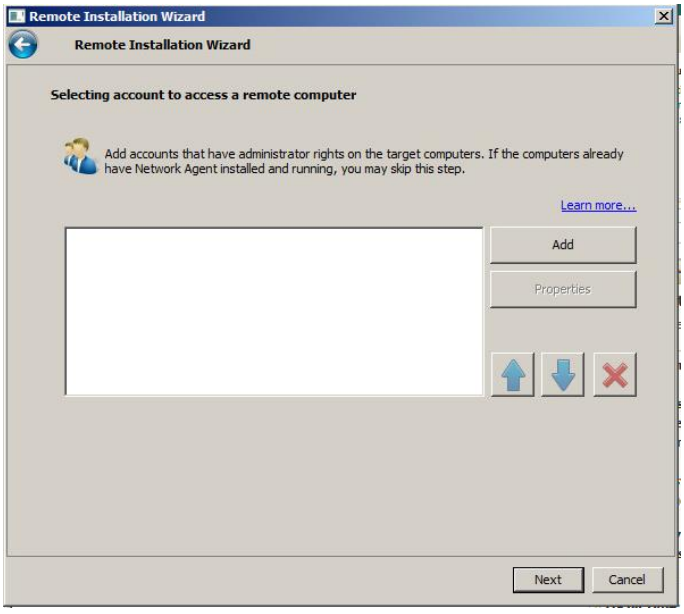


- Lưu ý: Chia sẻ máy in gồm 2 luật: 1 luật permit port 445, 139 theo TCP, 1 luật permit port 137, 138 theo UDP

+ Đối với máy tính VDI: phải mở thêm chiều inbound port 4172 (TCP/UDP), 32111 (TCP)

3.8. Cấu hình cài đặt phần mềm trên máy trạm

- Khi deploy 1 bộ cài trên máy trạm, tại bước chọn user lưu ý không chọn User nào cả, vì mặc định Net Agent trên máy trạm đã có quyền Administrators rồi.

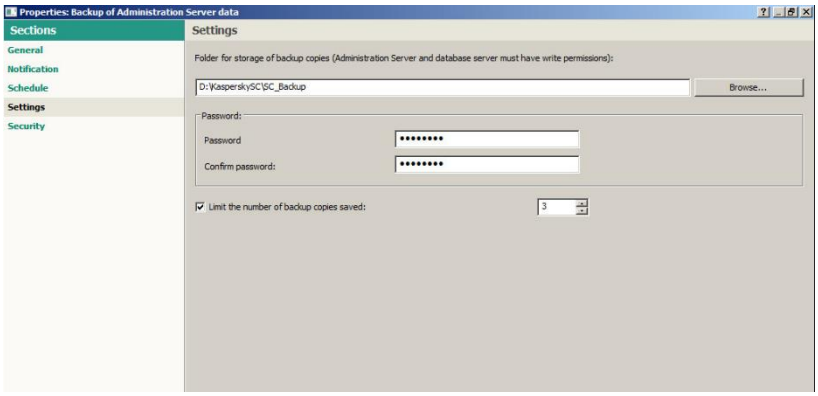


3.9. Cấu hình sao lưu cấu hình

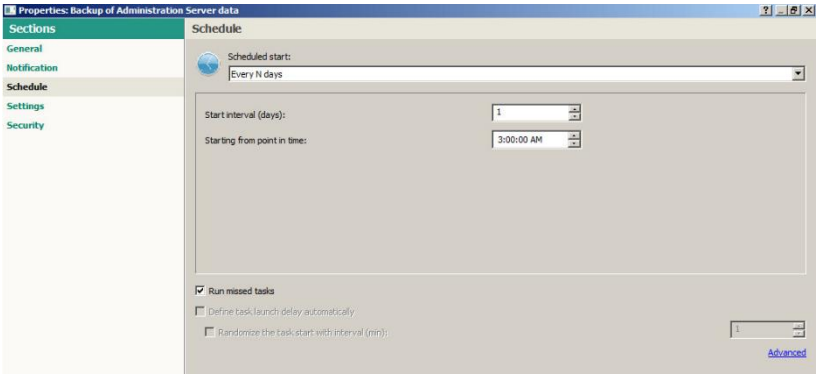
- Vào phần Administration Server Tasks.

- Nếu đã có task với task type: "Backup of Administration server data" rồi thì kiểm tra lại các tham số sau:

+ Settings: Chọn đường dẫn file backup (Lưu ý chọn nơi lưu trữ không cùng ổ đĩa với HĐH) và chọn password bảo vệ file backup và chọn lưu giữ tối thiểu 3 file backup gần nhất



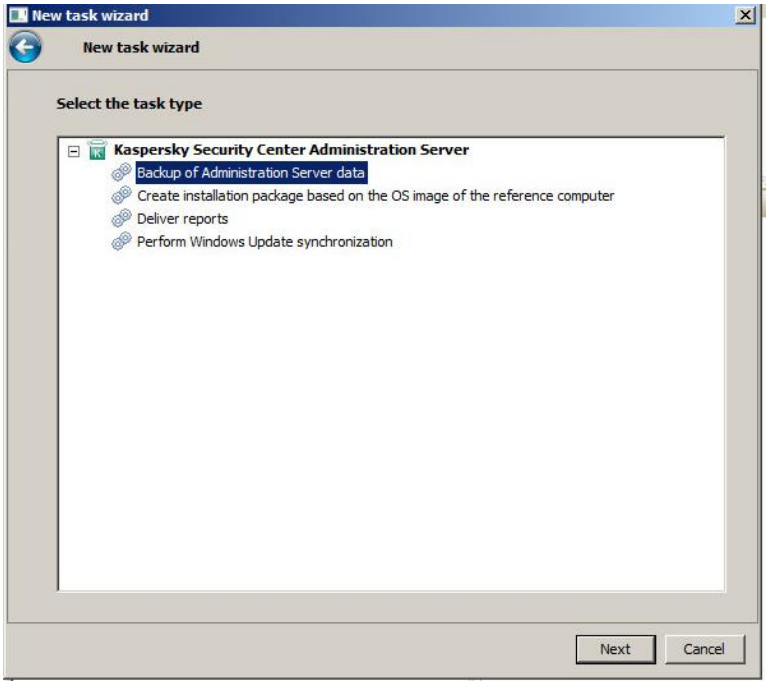
+ Shedule: Chọn thực hiện backup tối thiểu là hàng ngày



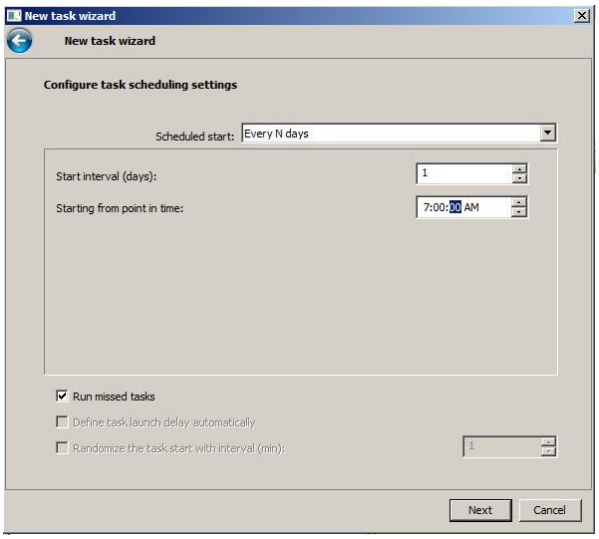
- Nếu chưa có task với task type task type: "Backup of Administration server data" thì tạo 1 task mới

+ Create New task

+ Chọn Task type là "Backup of Administration Server data"



+ Tất cả các option để mặc định. Sau đó chỉnh sửa lại các option theo như mục " Nếu đã có task với task type: "Backup of Administration server data"" phía trên.



4. Cấu hình lưu log

- Log Kaserskype Endpoint lưu ra windows event log.

- Cài đặt agent đẩy log windows event về server log tập trung theo hướng dẫn của agent

- Log phải được lưu thời gian theo quy định của đơn vị ban hành tiêu chuẩn

5. Yêu cầu giá ATTT định kỳ

- Đánh giá cấu hình dựa trên các hướng dẫn của phụ lục này

Phụ lục 13.
HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO HỆ THỐNG VPN SỬ DỤNG FIREWALL PALOALTO

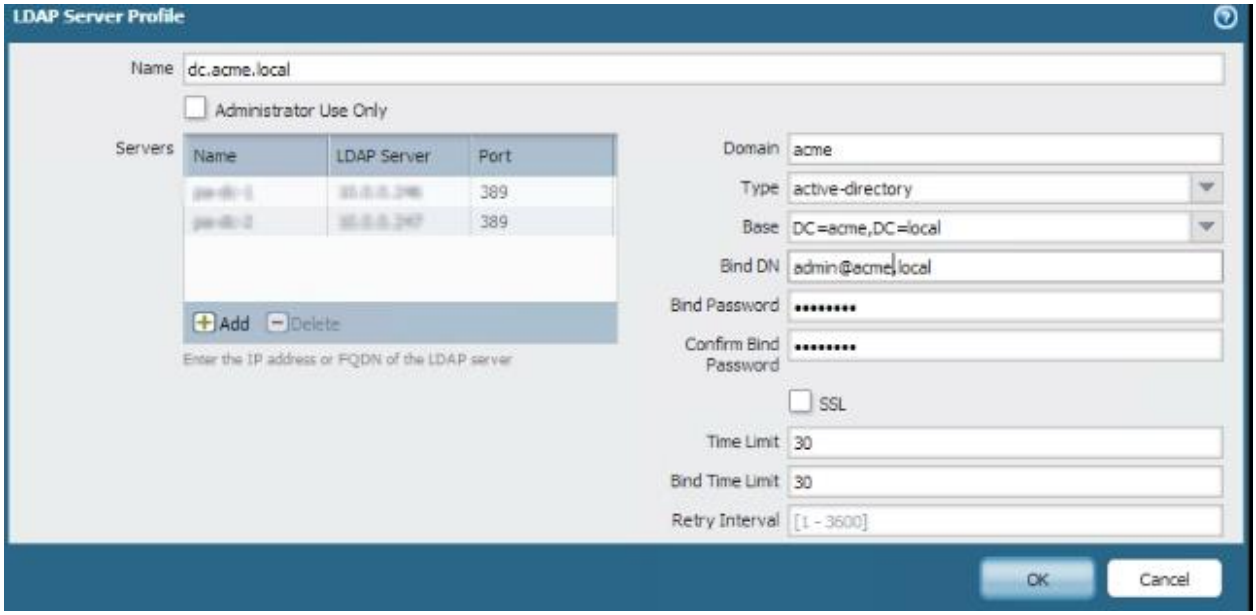
1. Đảm bảo tính xác thực

- Hệ thống VPN phải sử dụng phương pháp xác thực tập trung như TACACS, RADIUS, LADP…

- Cấu hình:

+ Cấu hình profile server để xác thực

o Chọn mục **Device > Server Profile > Có thể chọn LDAP, RADIUS…**



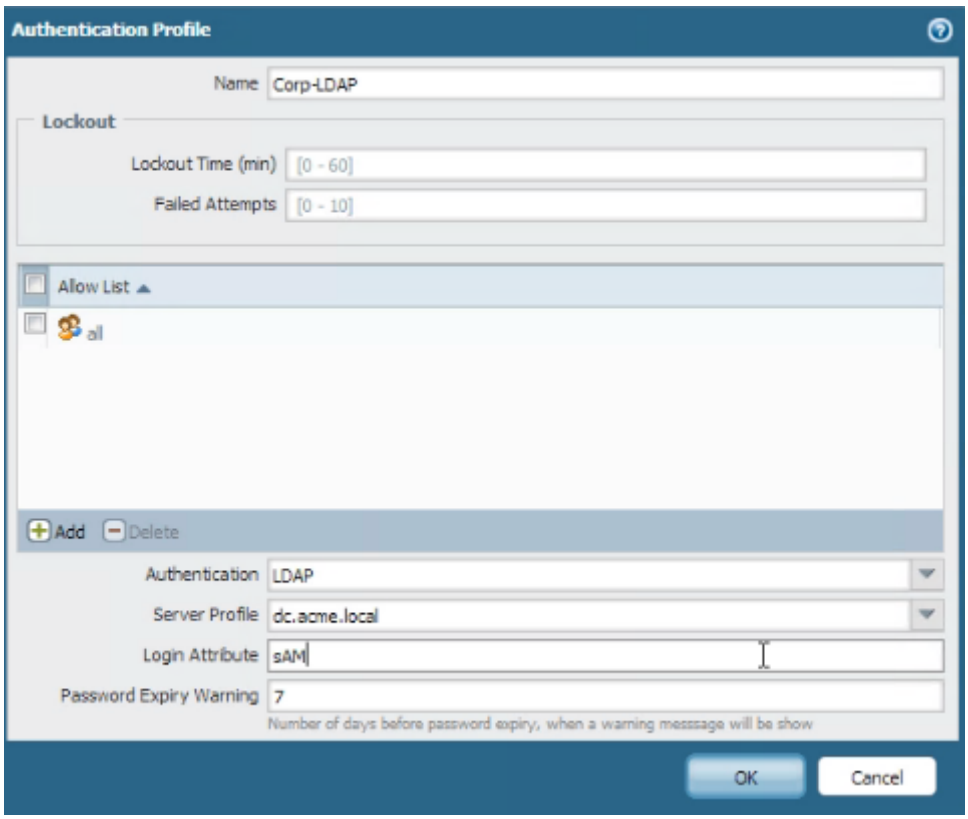
o Điền các thông tin cần thiết > **OK**

+ Cấu hình Authentication Profile

o Chọn mục **Device > Authentication Profile > Add**

o Trong **Authentication** chọn loại server **(LDAP, RADIUS…)**

o Trong **Server Profile** chọn Profile vừa tạo



- Click **OK** > Click Commit để apply cấu hình

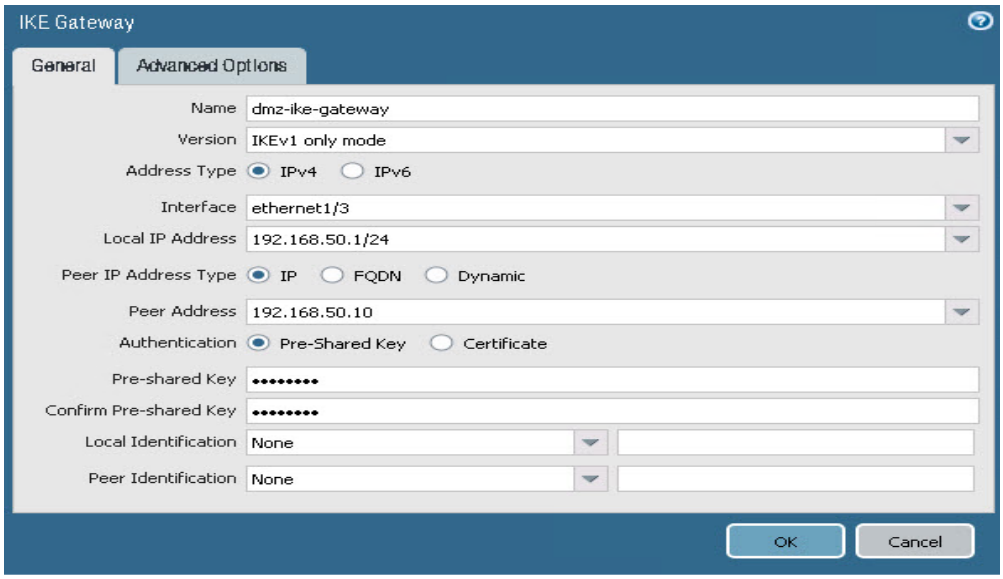
2. Nâng mức bảo mật lên mức cao nhất được hỗ trợ

2.1. Đối với VPN site to site

- Cấu hình:

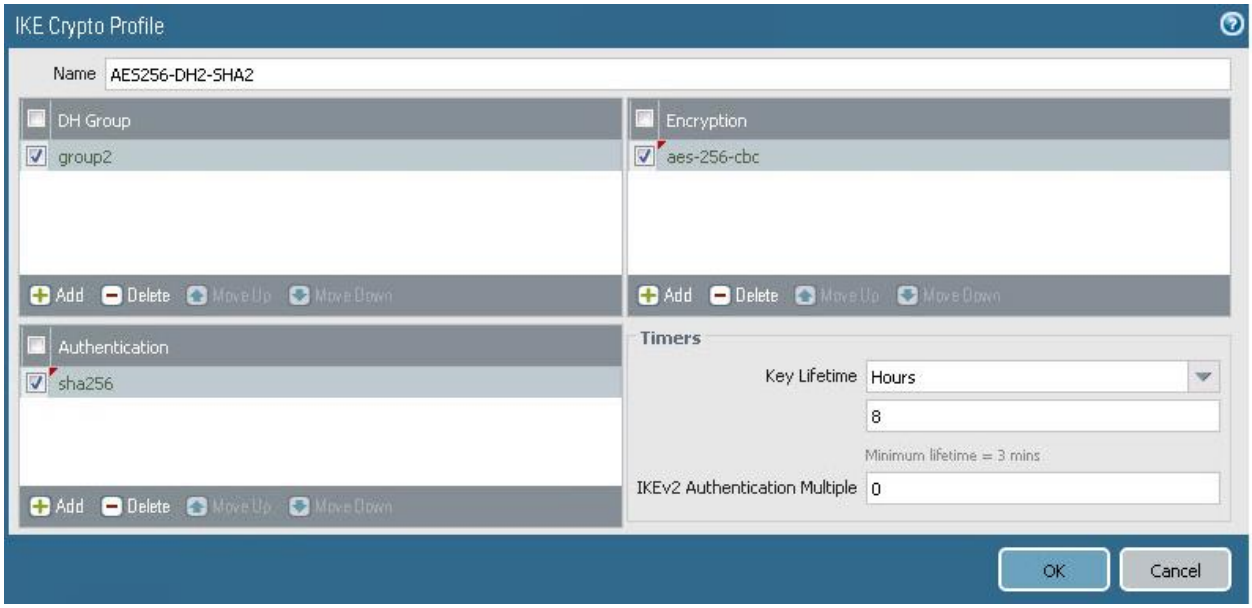
+ Cấu *hình IKE Crypto Profile cho IKE Gateway*

- Chọn mục **Network > Network Profiles > IKE Gateways > Click Add** để tạo mới hoặc chọn IKE gateway đã có sẵn



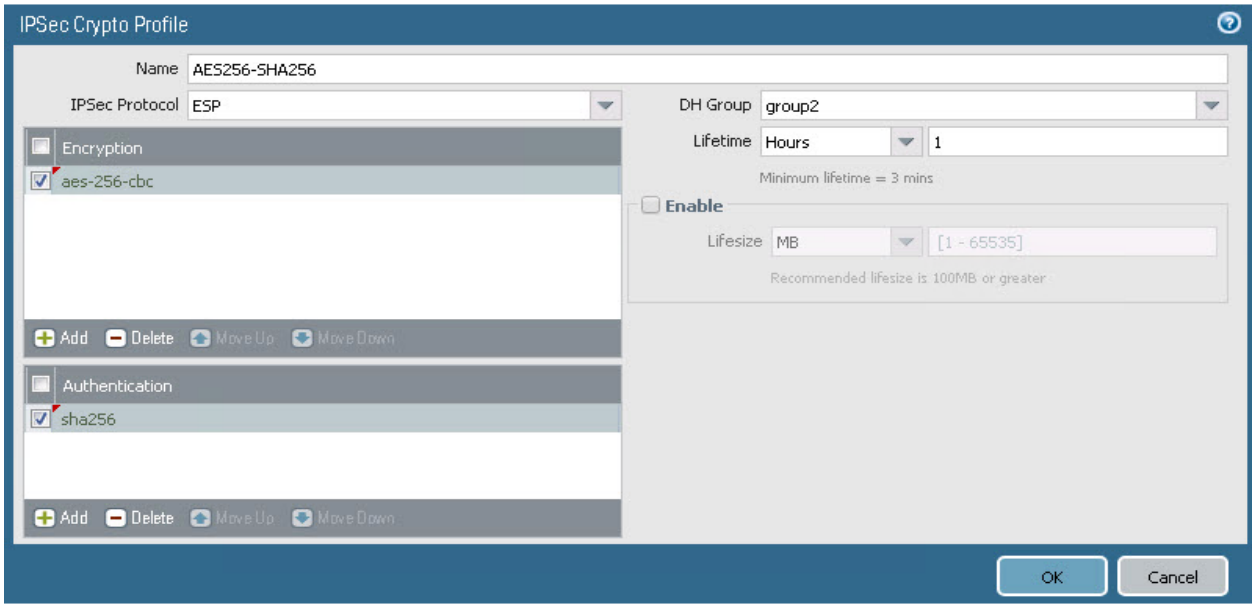
- Chọn các thông số cần thiết > **Advanced Options**

- Trong tab **IKEv1 > IKE Crypto Profile >** chọn các thông số như sau:
- DH Group: Add Group 2
- Authentication: add sha256
- Encryption: Add aes-256-cbc



- Click **OK 2 lần** để lưu cấu hình

+ *Tạo* IPsec *Crypto Profile*
  - Chọn mục **Network > Network Profiles > IPSec Crypto > Click Add >** chọn các thông số như sau **> OK**
  - IPSec Protocol: ESP
  - Encryption: Add aes-256-cbc
  - Authentication: Add sha256
  - Dh Group: chọn group 2



+ *Gán* IPSec *profile vào Tunnel*

  - Chọn mục **Network > IPSec Tunnel > Click Add** để thêm mới hoặc chọn Tunnel đã có sẵn
  - Trong IKE Gateway chọn Gateway đã cấu hình profile ở
  - Trong IPSec Crypto Profile chọn Profile vừa tạo ở trên.

  - Click **OK** > Click

để apply cấu hình
  - Kiểm tra: Trong mục tương tự

2.2. Đối với SSL VPN Client to Site (Global Protect)

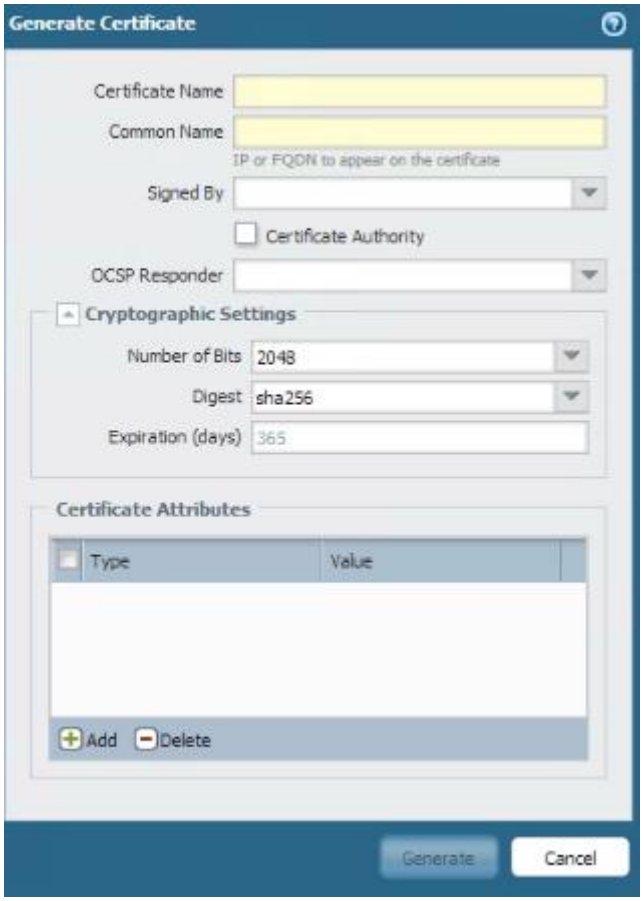
- Cấu hình mã hóa Certificate. (Trong trường hợp FW làm server khởi tạo cert)

+ Cấu hình:

- Chọn mục **Device > Device Certificate > Generate**
- Trong **Cryptographic Settings:** Chọn các thông số như sau > Click **Generate**

  Number of Bits: 2048 trở lên

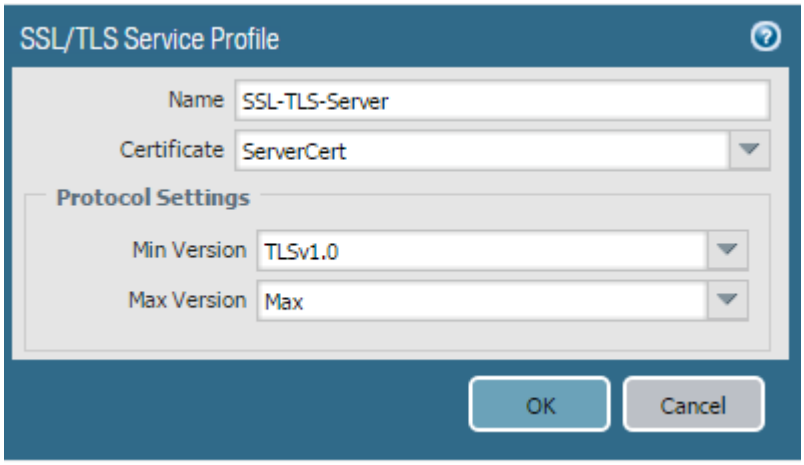
  Digets: sha256



- Kiểm tra: Trong mục tương tự

- Cấu hình SSL/TLS service profile

+ Cấu hình:
  - Chọn mục **Device > Certificate Management > SSL/TLS Service Profile**



- Trong **Certificate**: Chọn Certificate đã tạo ở trên hoặc Certificate bên thứ 3 đã được import.
- **Min version**: Chọn **TLSv1.2**
- **Max version**: Chọn **Max**
- Click **OK** > Click Commit để apply cấu hình
- Kiểm tra: Trong mục tương tự

3. Kiểm soát kết nối

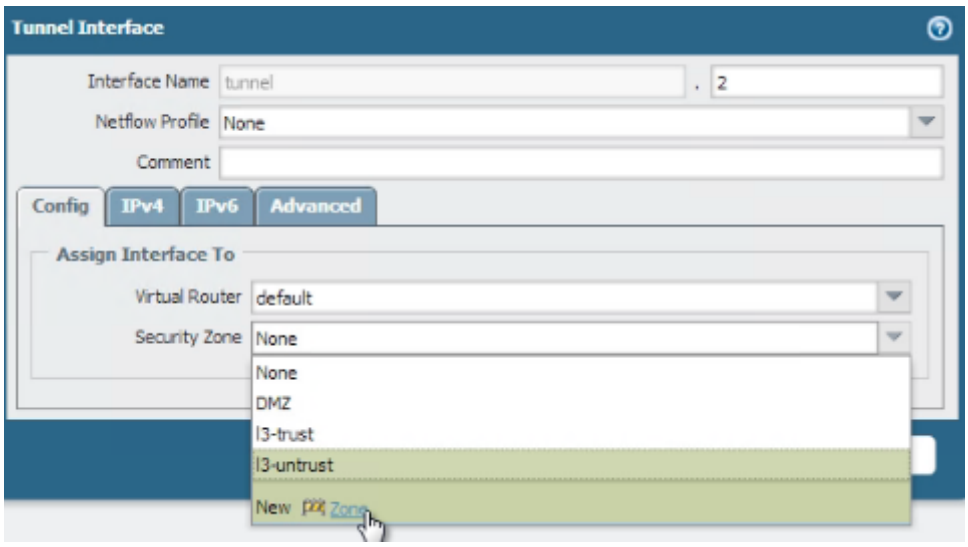
3.1. Khai báo rule phát hiện và chặn kết nối port quản trị , port kết nối đến database...

- Palo Alto có rule mặc định interzone-default chặn kết nối giữa các zone với nhau.

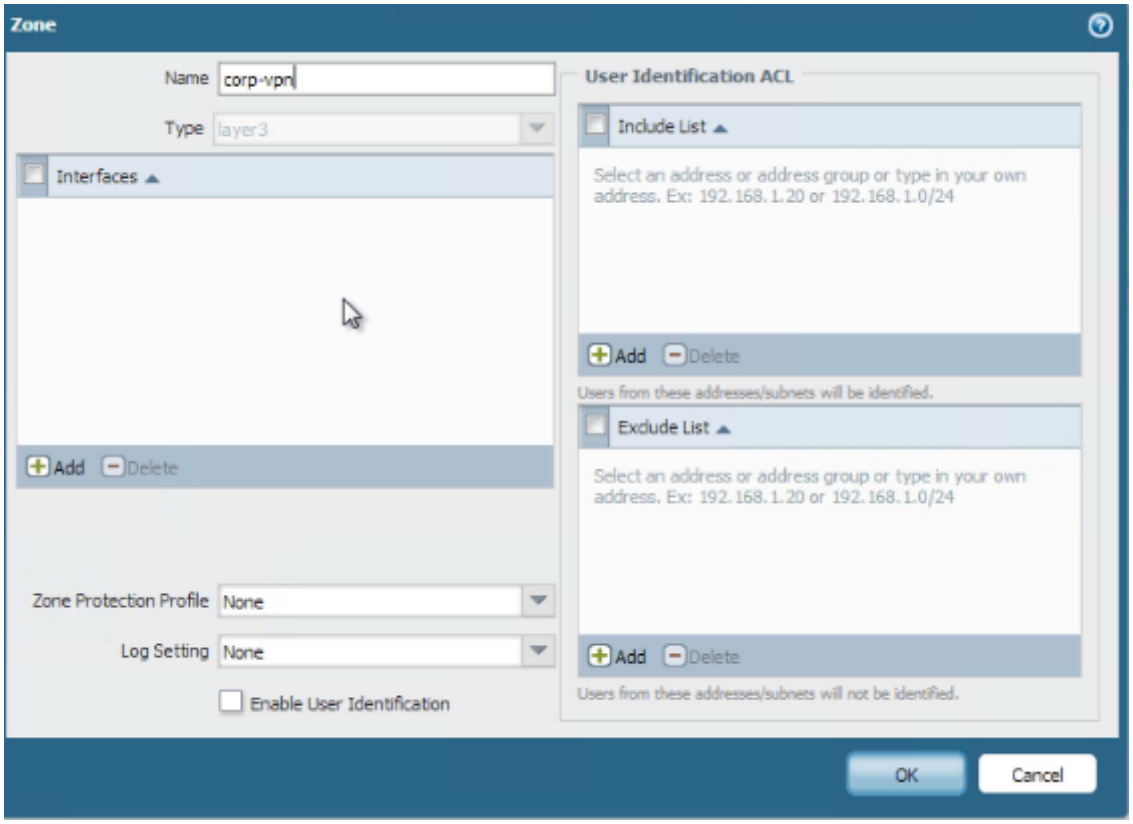
- Interface tunnel VPN cần được cấu hình vào 1 zone riêng biệt
- Cấu hình

+ Chọn mục **Network** > **Interfaces** > **Tunnel** > **Click Add** để tạo mới hoặc chọn Tunnel interface đã tạo sẵn

+ Trong tab **Config** > **Security Zone** > chọn **New**



+ Trong tab **Config > Security Zone** > chọn **New**



+ Điền **Name** > tick chọn **Enable User Identification** > **OK** > **OK**

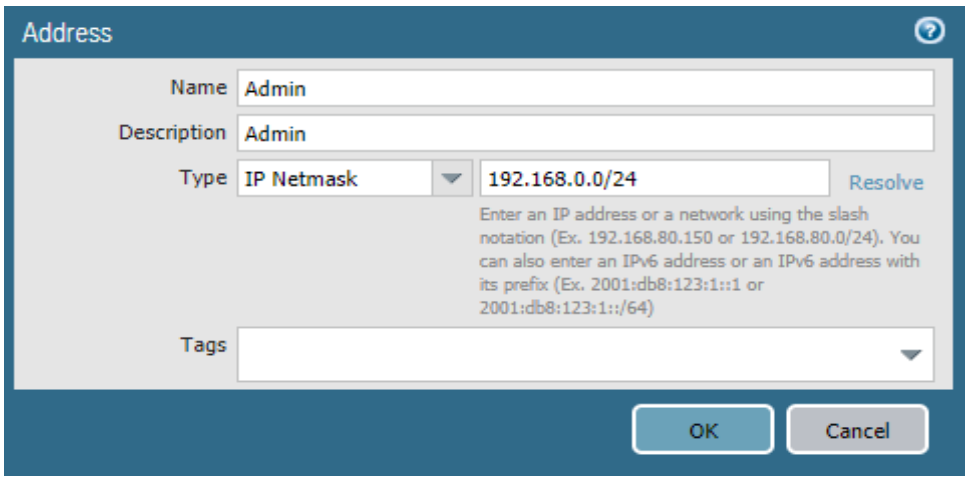
+ Click Commit để apply cấu hình

3.2. Yêu cầu rule khai báo Policy mở kết nối chính xác các địa chỉ nguồn, địa chỉ đích và port dịch vụ

- Cấu hình

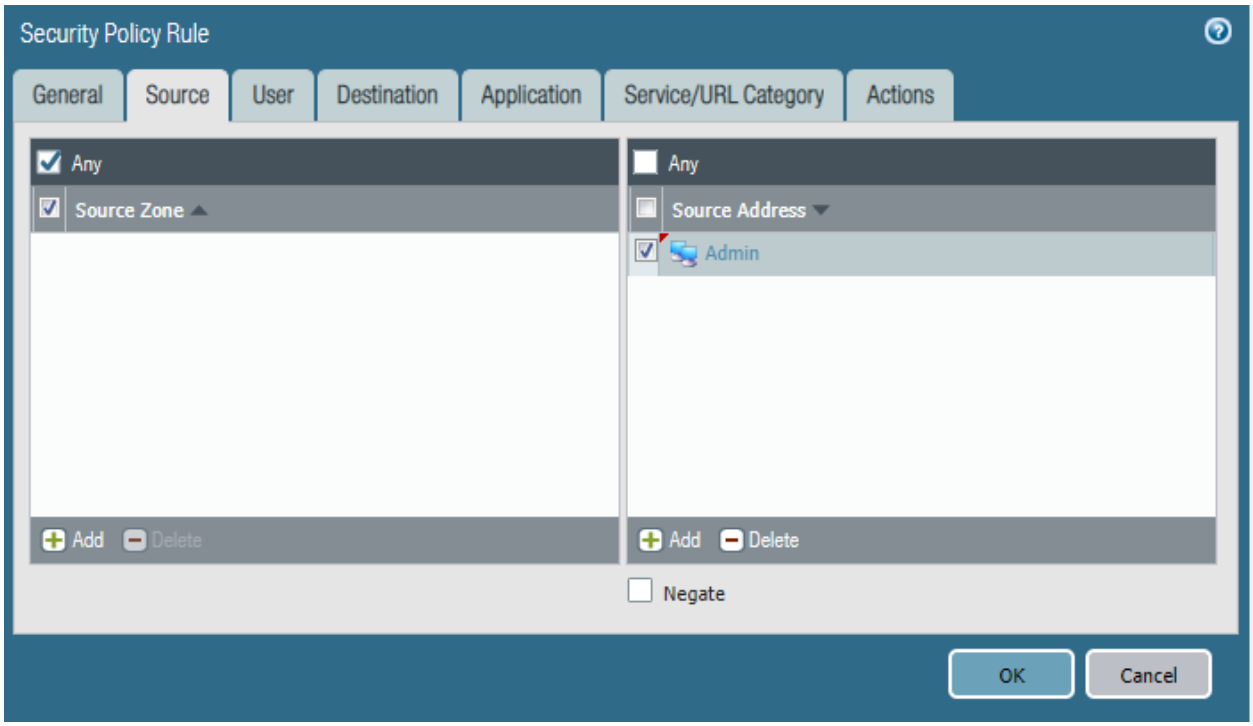
+ Tạo Address dải IP VPN

  - Chọn mục **Objects > Address > Add**



- Điền dải IP VPN > **OK**

+ Khai báo Policy
  - Chọn mục **Policies > Security > Add**
  - **Tab General: Rule Type** chọn **universal**
  - **Tab Source: Source Zone** chọn **Zone VPN, Source Address** chọn **Address VPN** vừa tạo.



  - **Tab Destination: Destination Zone** chọn các Zone nội bộ cần kết nối **, Destination Address** chọn chính xác IP cần kết nối. Không mở theo range
  - **Tab Application** và **Service** chọn chính xác các port service cần kết nối. Không mở thep range
  - **Tab Action:** chọn **allow,** tick chọn **Log at Session Start > OK > Click** để apply cấu hình

- Kiểm tra: Trong mục tương tự

4. Tắt các tính năng hỗ trợ không đảm bảo an toàn

- Chỉ bật các tính năng hỗ trợ đã đảm bảo an toàn và thống kê các tính năng này trong checklist để đánh giá chỉ bật lên khi có yêu cầu sử dụng

5. Yêu cầu môi trường vận hành an toàn (với hệ thống phần mềm VPN triển khai trên các máy chủ)

- User remote quản trị hệ thống phải enable cơ chế xác thực đa nhân tố (token/OTP).

- Sử dụng 1 máy riêng đảm bảo toàn bộ các tiêu chuẩn ATTT cho máy người dùng cuối để vận hành hệ thống .

- Sử dụng các máy riêng để vận hành hệ thống, không dùng cho các công việc thông thường hàng ngày (Duyệt email, truy cập internet, đọc file văn bản MSOffice/pdf.

Phụ lục 14.
HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO THIẾT BỊ FIREWALL

I. Hướng dẫn cho firewall PALO ALTO

1. Yêu cầu chung

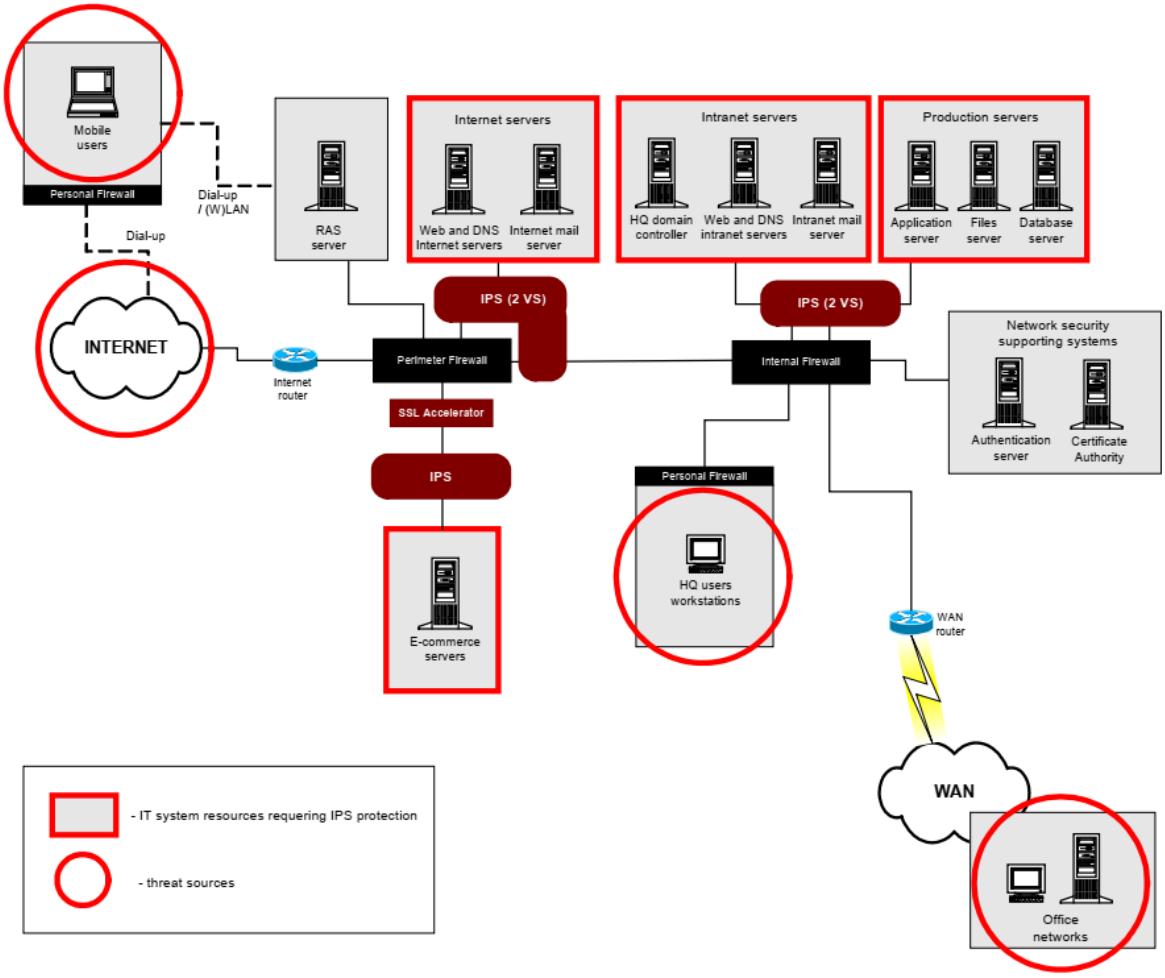
1.1. Yêu cầu phát hiện và chống tấn công từ internet

- Phải đặt IPS/IDS tại các vùng mạng mà monitor được tất cả các traffic in/out internet

  - Đặt tại vùng DMZ kết nối internet
  - Đặt tại vùng người dùng truy cập Internet.

- Phải đặt Firewall giữa kết nối từ Internet vào mạng nội bộ, đảm bảo toàn bộ traffic in/out internet phải đi qua Firewall

  - Đặt tại vùng DMZ kết nối internet
  - Đặt tại vùng người dùng truy cập Internet.



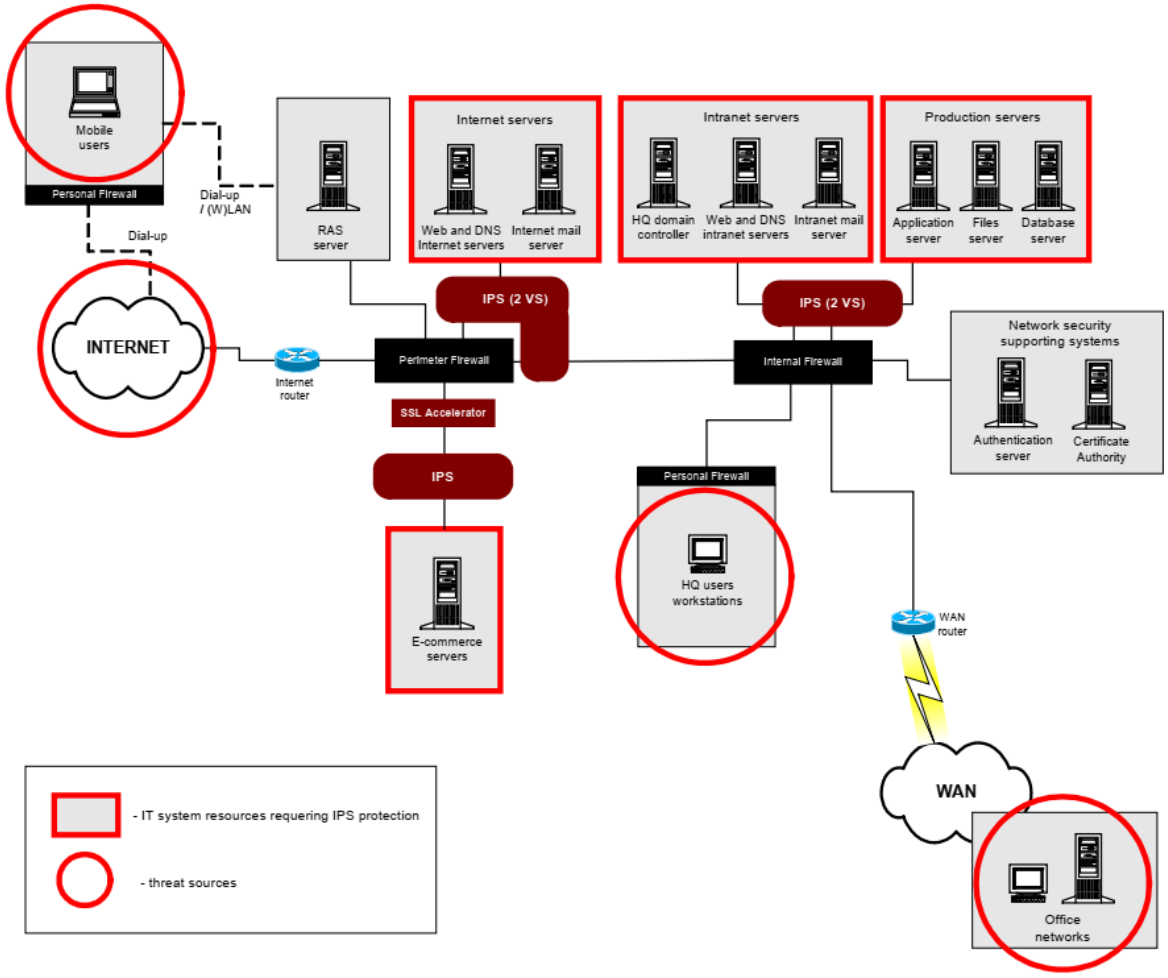
1.2. Yêu cầu phát hiện và chống tấn công từ nội bộ

- Phải đặt IPS/IDS tại các vùng mạng mà monitor được tất cả traffice in/out các hệ thống cần bảo vệ

  - Đặt tại vùng Office kết nối vào mạng nội bộ.
  - Đặt tại vùng WAN kết nối vào mạng nội bộ.
  - Đặt tại vùng Server Farm kết nối vào mạng nội bộ.
  - Đặt tại vùng Partner kết nối vào mạng nội bộ.

- Phải đặt Firewall giữa kết nối từ các hệ thống khác tới hệ thống cần bảo vệ, đảm bảo toàn bộ traffic in/out của vùng mạng cần bảo vệ đi qua Firewall

  - Đặt tại vùng Office kết nối vào mạng nội bộ.
  - Đặt tại vùng WAN kết nối vào mạng nội bộ.
  - Đặt tại vùng Server Farm kết nối vào mạng nội bộ.
  - Đặt tại vùng Partner kết nối vào mạng nội bộ.

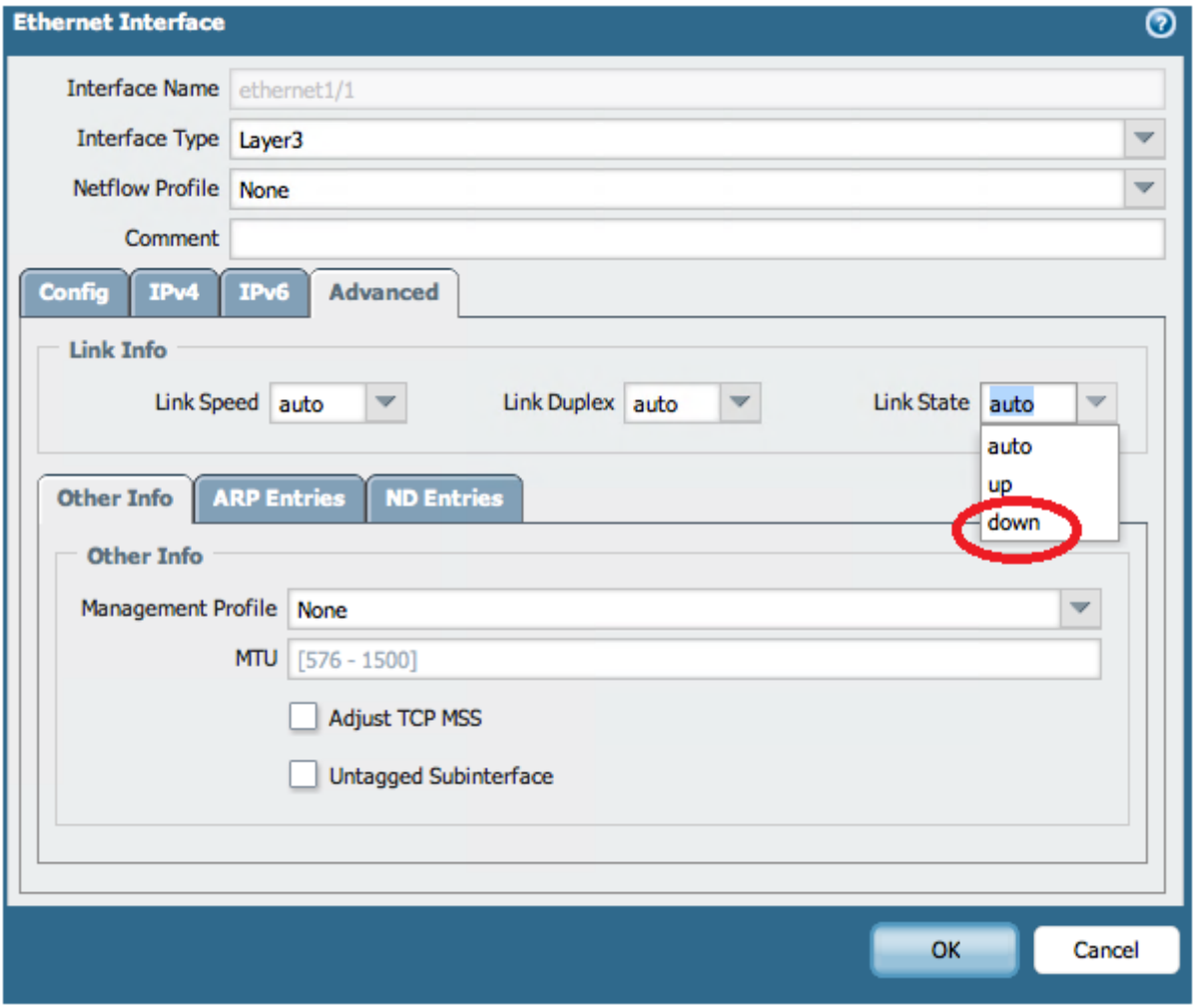


2. Cấu hình an ninh lớp 1

2.1. Yêu cầu shutdown port không sử dụng

- Shutdown tất cả các port không sử dụng trên thiết bị, chỉ bật lên khi có yêu cầu sử dụng

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Network > Interface**
    - Chọn Interface muốn shutdown



    - Trong tab **Advanced > Link State** chọn **down**
    - Click **OK > Click** để apply cấu hình

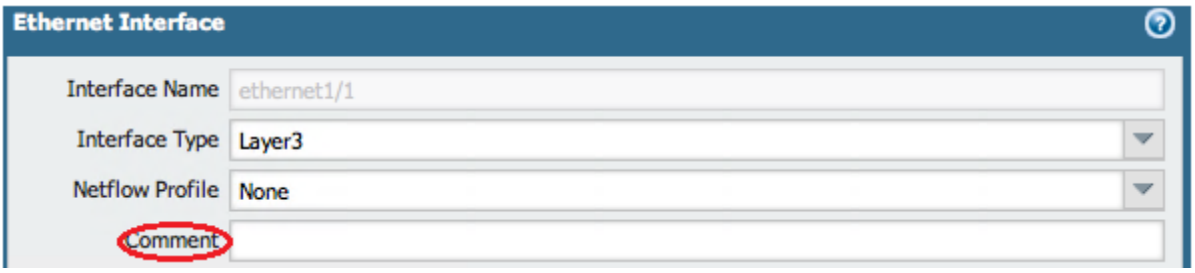
  - Kiểm tra: Trong mục tương tự

2.2. Yêu cầu mô tả kết nối rõ ràng

- Cổng đang bật phải có mô tả kết nối rõ ràng xác định được thông tin đấu nối của thiết bị đầu xa

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Network > Interface**
    - Chọn Interface muốn thêm mô tả

- Nhập mô tả vào ô **Comment** > **OK** > Click Commit để apply cấu hình



- Kiểm tra: Trong mục tương tự

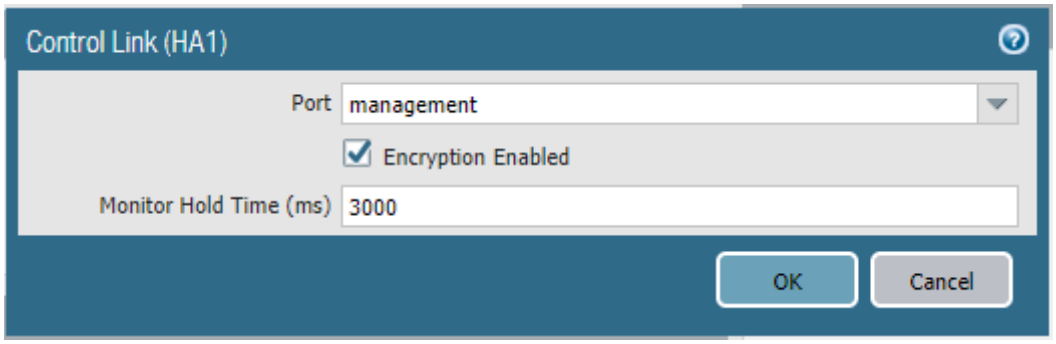
3. Cấu hình an ninh lớp 3

3.1. Xác thực cho các giao thức lớp 3

- VRRP, HSRP, GLBP, NSRP phải cấu hình xác thực cho giao thức giữa các thiết bị

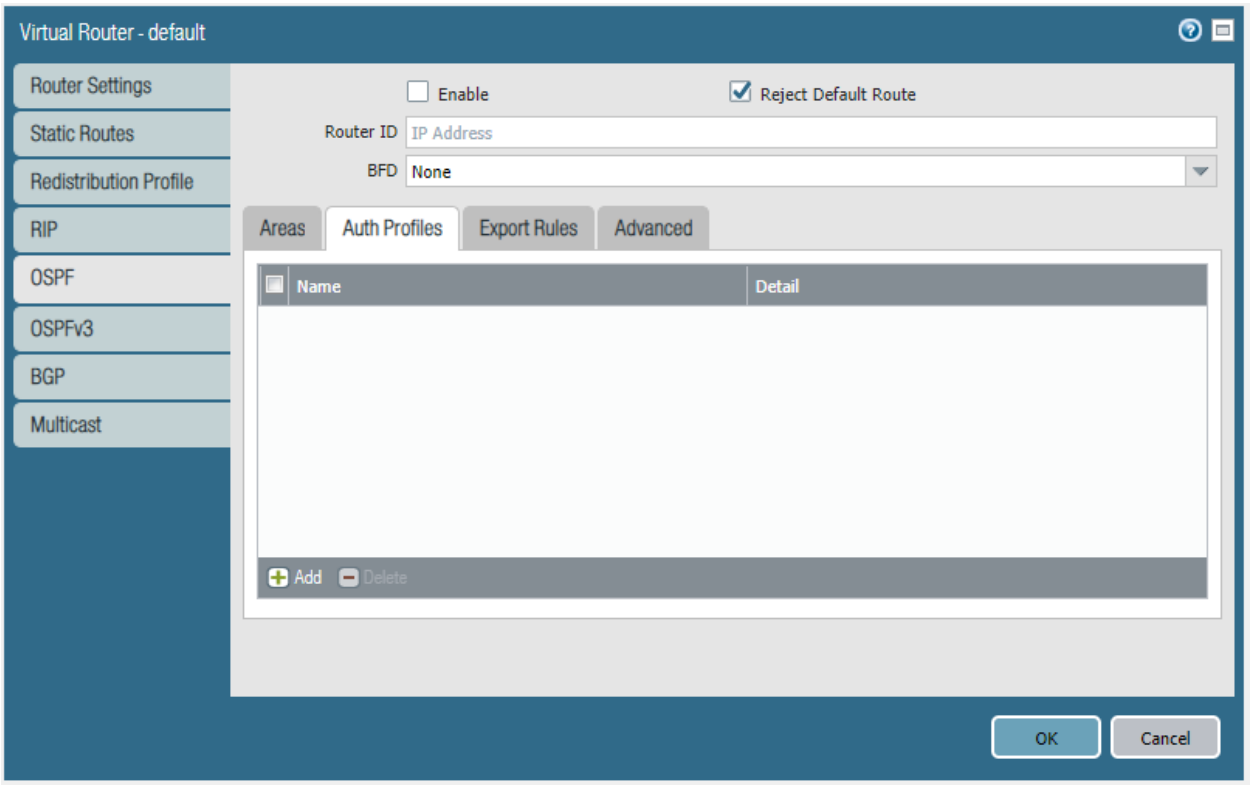
Firewall Palo Alto không hỗ trợ riêng từng giao thức VRRP/HSRP/GLBP/NSRP mà sử dụng mô hình HA để backup giữa 02 Firewall.

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Device** > **High Availability** > **Control Link (HA1)**
    - Tick chọn **Encryption Enabled** > **OK**> Click Commit để apply cấu hình

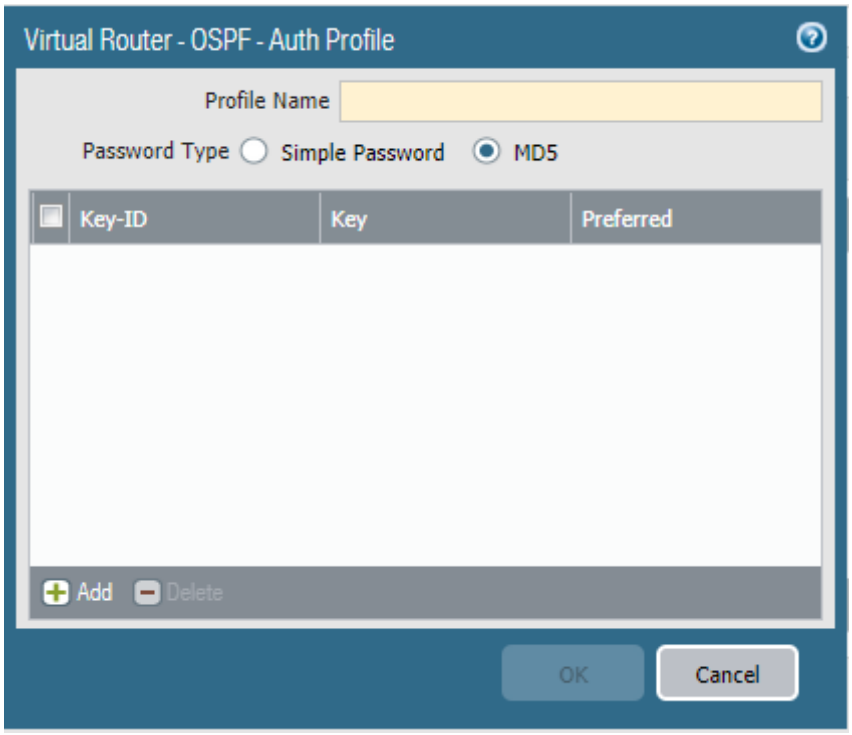


  - Kiểm tra: Trong mục tương tự

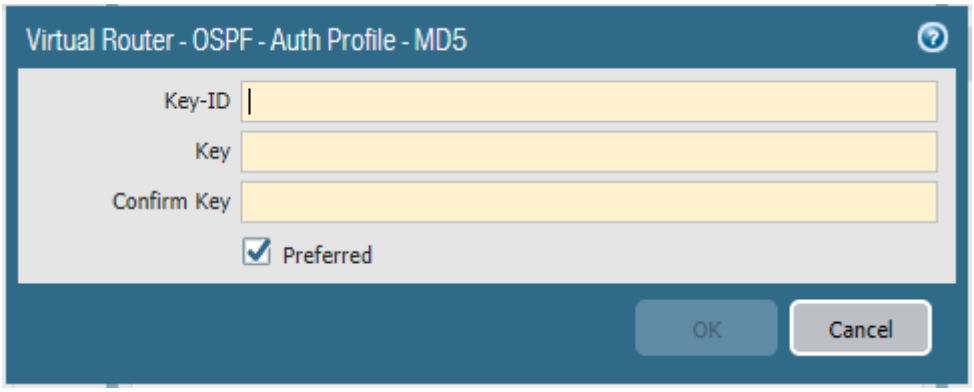
- OSPF phải thiết lập chuỗi xác thực có mã hóa giữa 2 thiết bị
  - Trên GUI:
    - Cấu hình:
      - Chọn mục **Network** > **Virtual Router** > Chọn tên của Virtual Router đang sử dụng > **OSPF**



- Chọn tab **Auth Profiles** > **OSPF** > Click **Add**



- Điền **Profile Name** > Tick chọn **MD5** > Click **Add**



- Điền **Key ID và Key** > Click **OK** > Click Commit để apply cấu hình

- Kiểm tra: Trong mục tương tự

4. Cấu hình quản trị

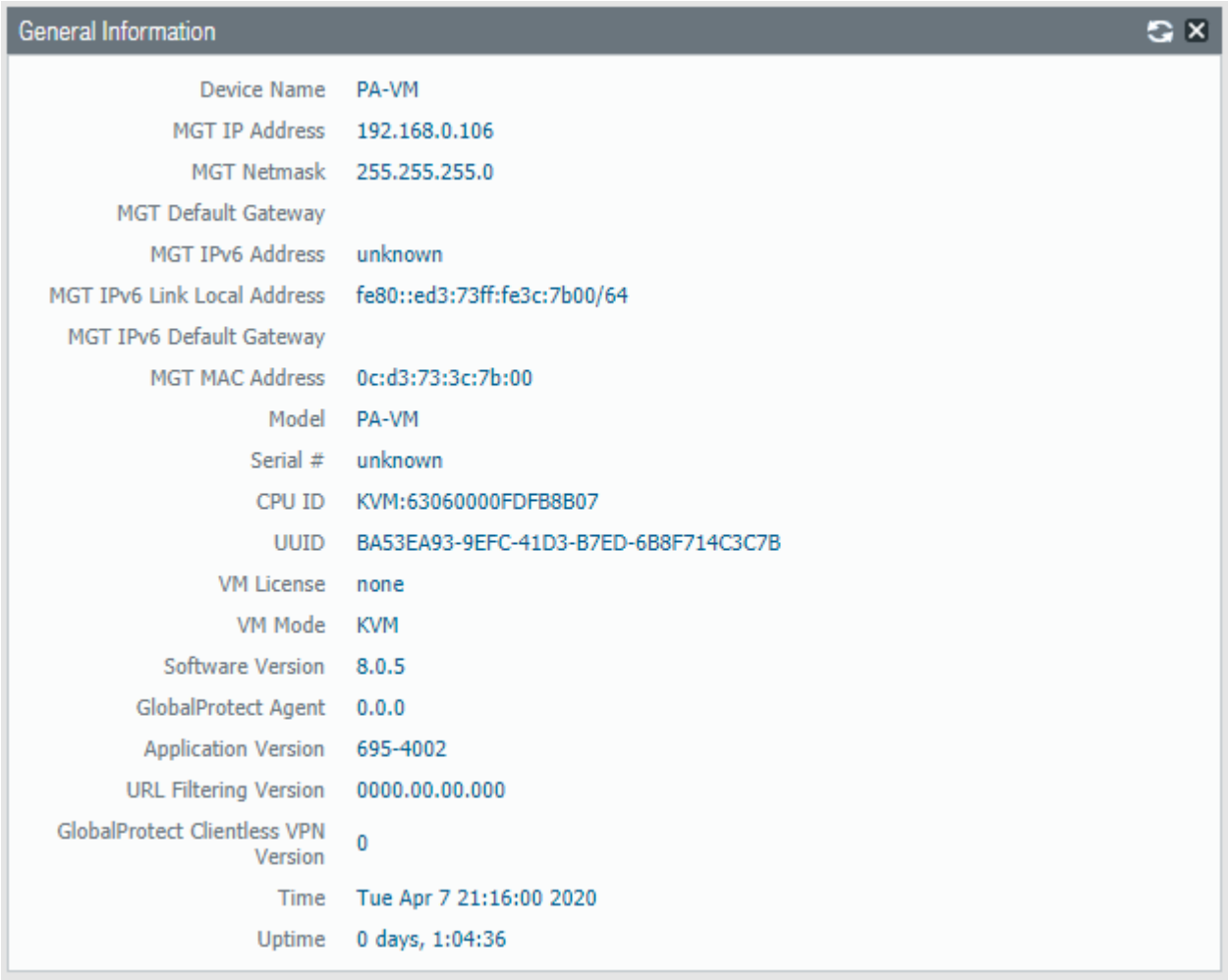
4.1. Yêu cầu về sao lưu cấu hình

- Thiết bị phải được sử dụng phiên bản hệ điều hành và cập nhật các bản vá đảm bảo an toàn theo yêu cầu của bộ phận ATTT.

- Trên GUI:

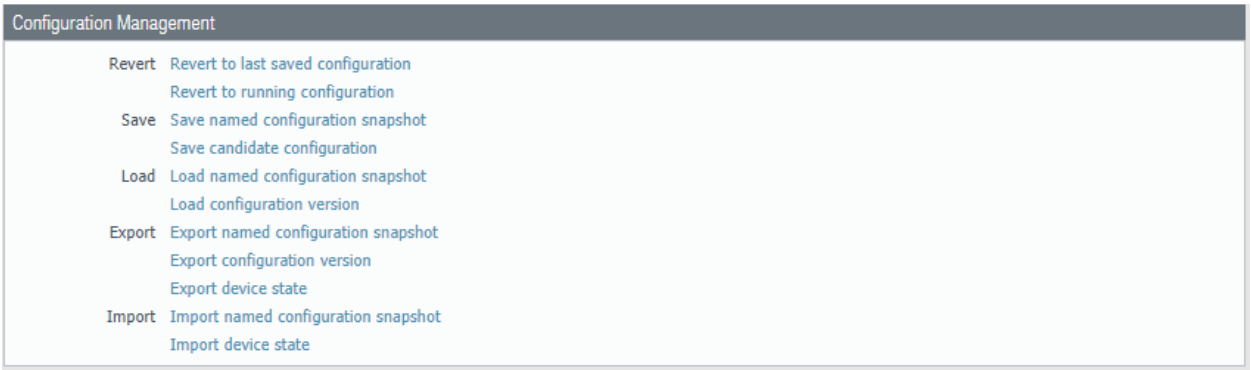
- Kiểm tra:

- Chọn mục **Dashboard** > **General Information**

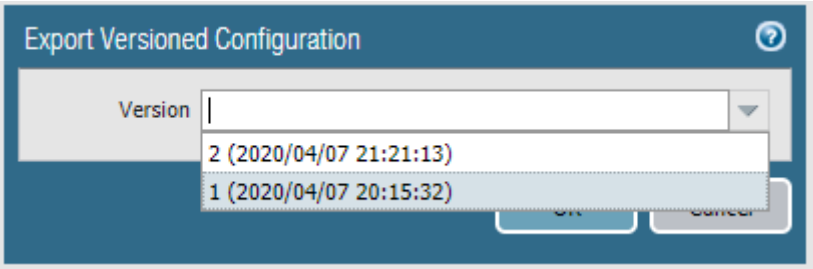


- Lưu cấu hình trước khi tác động và định kì tối thiểu 01 lần/tuần. Lưu tối thiểu 02 bản gần nhất. Không lưu bản sao lưu trên máy tính cá nhân của quản trị viên.

- Trên GUI:
  - Cấu hình:
  - Backup thủ công:
    - Chọn mục **Device > Setup > Operations > Configuration Management**



- Click **Export configuration version > Chọn bản mới nhất > OK > Click** Commit để apply cấu hình

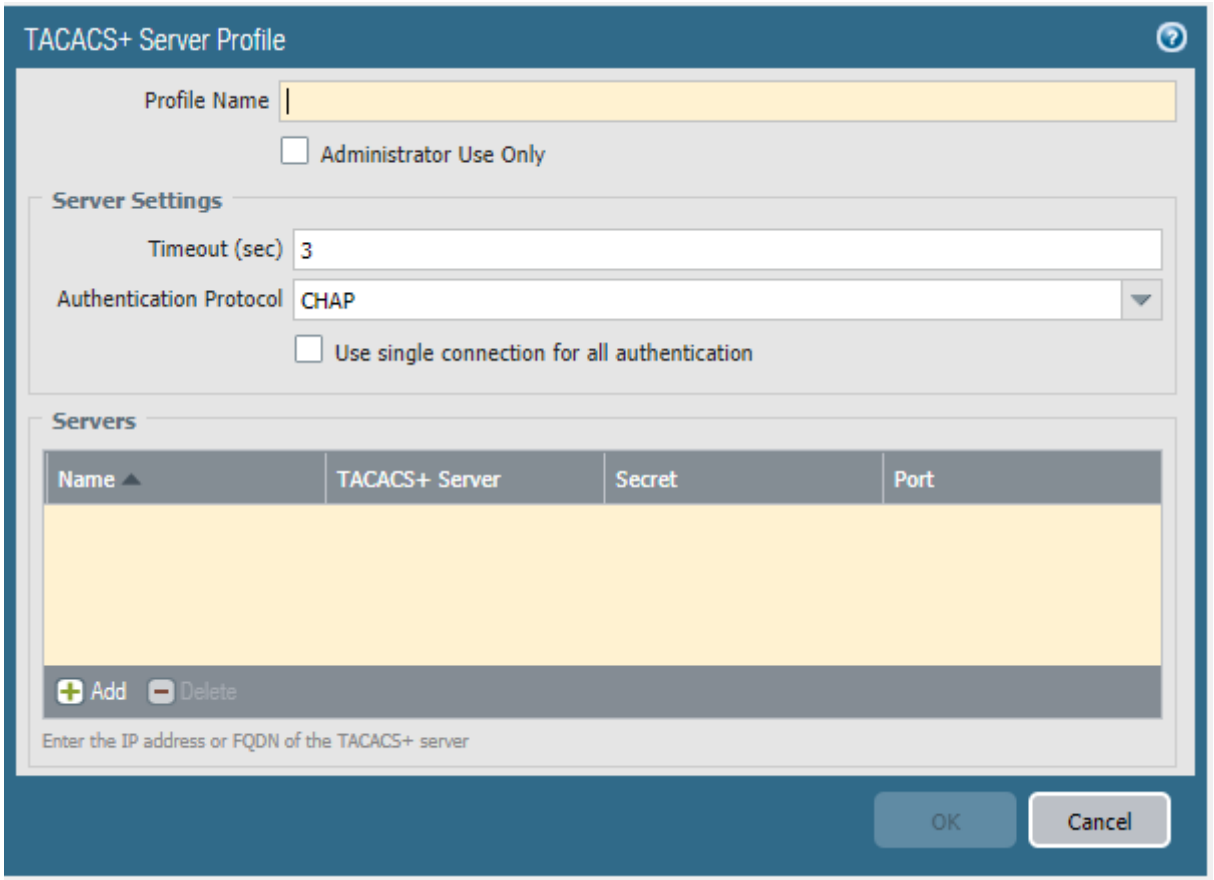


- Backup tự động: Yêu cầu phải có máy chủ Panorama
- Kiểm tra: Kiểm tra file cấu hình được lưu trên máy tính đích.

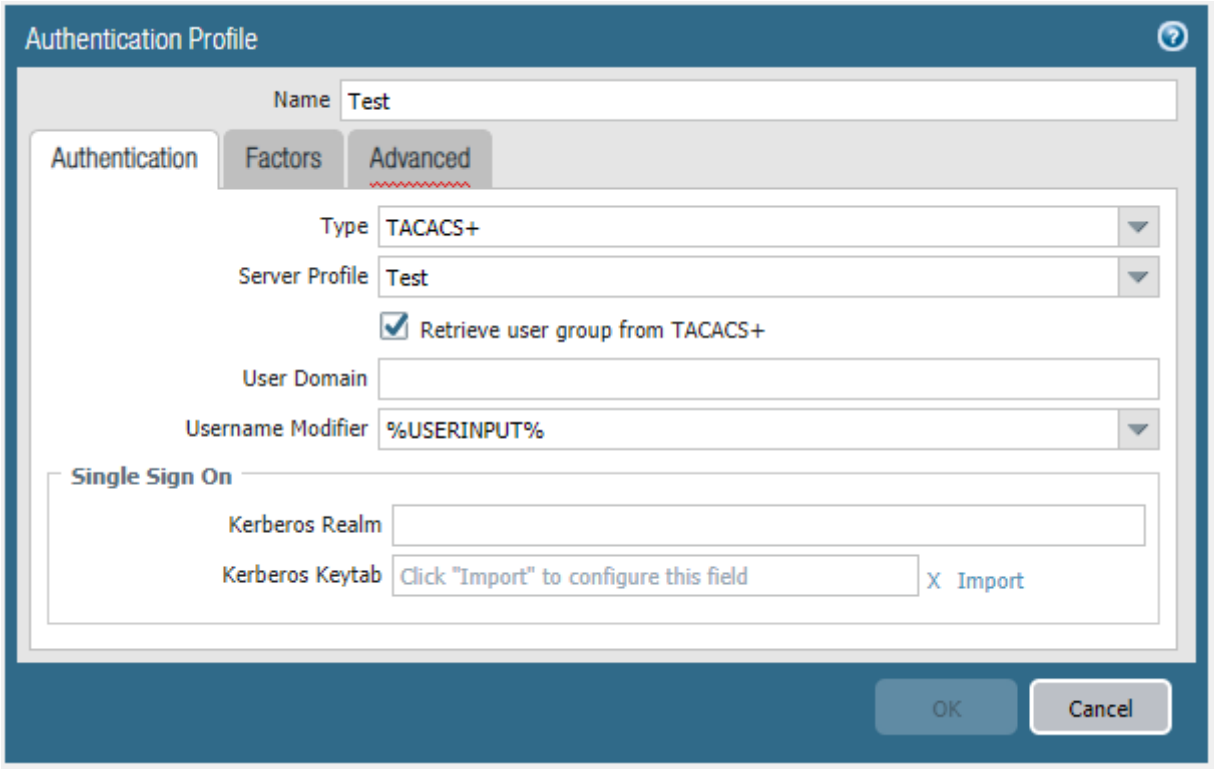
4.2. Yêu cầu về quản lý tài khoản

- Sử dụng hệ thống AAA để quản lý tài khoản người dùng tập trung (xác thực, phân quyền, ghi lịch sử tác động). Tối đa 02 tài khoản quản trị local dùng cho trường hợp khẩn cấp

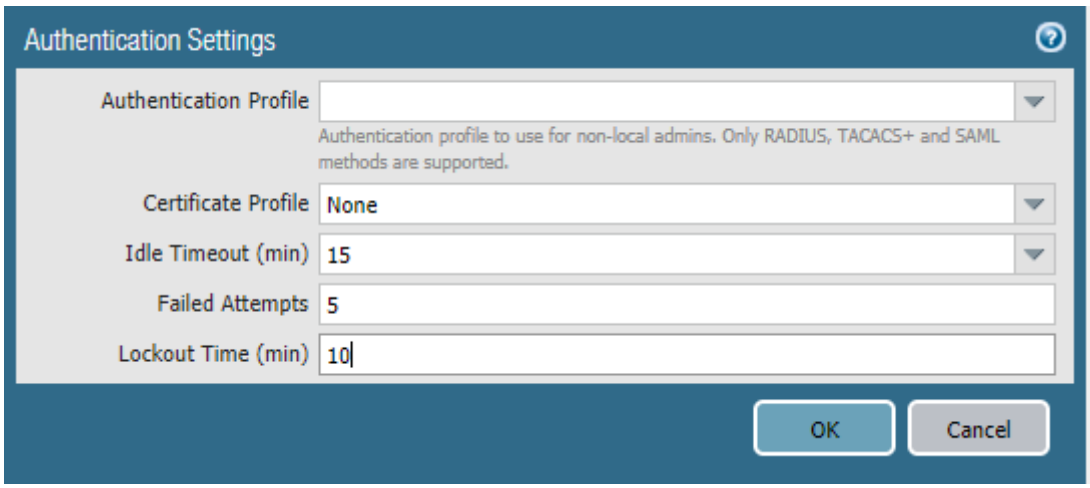
- Trên GUI:
  - Cấu hình:
    - Chọn mục **Device > Server Profile** > Có thể chọn 1 trong các kiểu svr AAA tùy nhu cầu: **Radius, Tacacs+, Kerberos...** > Click **Add**



- Nhập các thông số của AAA Server > **OK**
- Chọn mục **Device > Authentication Profile** > Click **Add**



- **Type** và **Server profile** chọn theo profile vừa tạo ở trên > tick chọn **Retrieve user group from... > OK.** Có thể config thêm yếu tố xác thực ở tab **Factor** và giới hạn các user truy cập trong tab **Advance**
- Chọn mục **Device > Setup > Management > Authentication Settings >** Click vào biểu tượng để edit



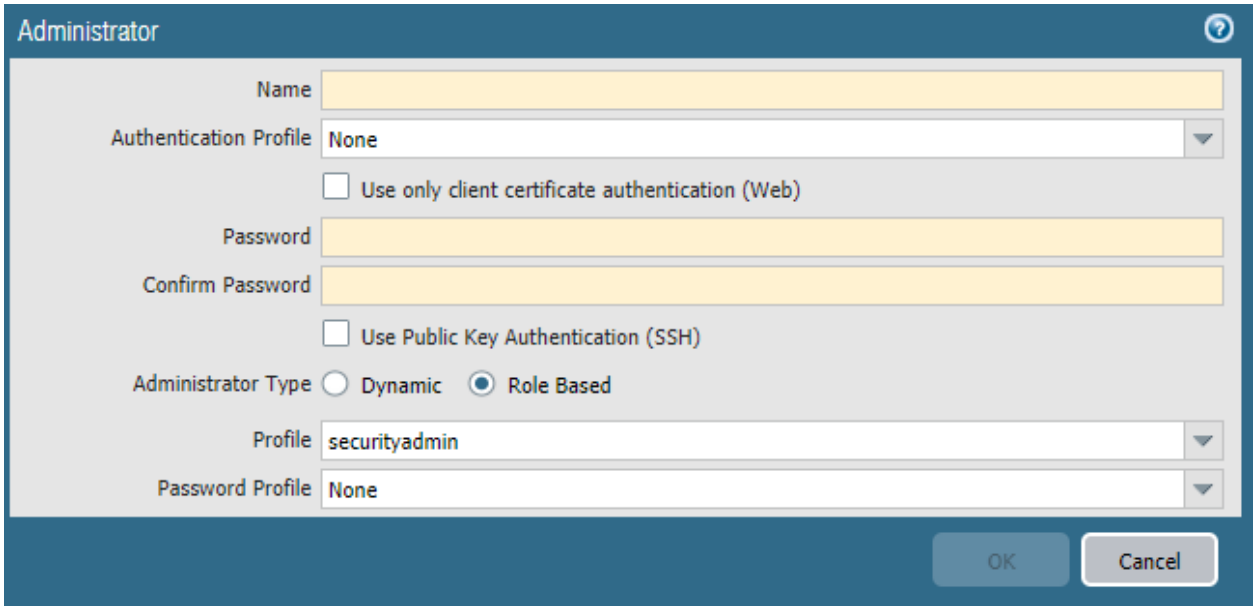
- **Authentication Profile**: chọn profile vừa tạo > Điền các tham số như dưới > **OK**

  Idle Timeout: 15 min

  Failed Attempts: 5

Lockout Time: 10

- Tạo user local: Chọn mục **Device > Administrator**



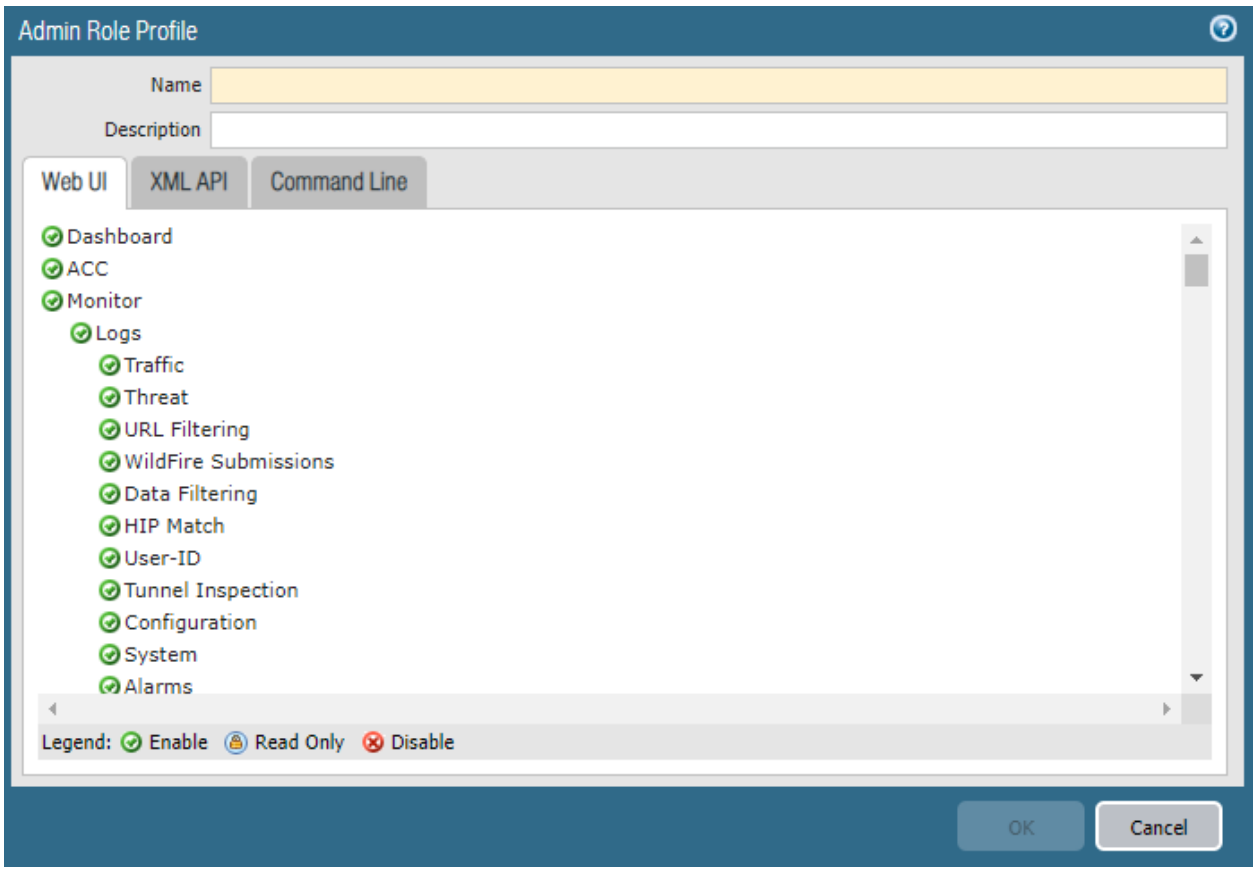
- Điền các thông tin > **Administrator Type: chọn Role Based >** chọn Profile thích hợp có sẵn(audit, crypto, security) hoặc tự tạo profile theo ý muốn > **OK > Click** Commit để apply cấu hình

- Kiểm tra: Trong mục tương tự

- Quản trị viên phải sử dụng tài khoản được cấp riêng, phân quyền phù hợp trên local/AAA

Đối với tài khoản Local

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Device > Admin Role > Add**
    - Chọn các quyền thích hợp cho **User**

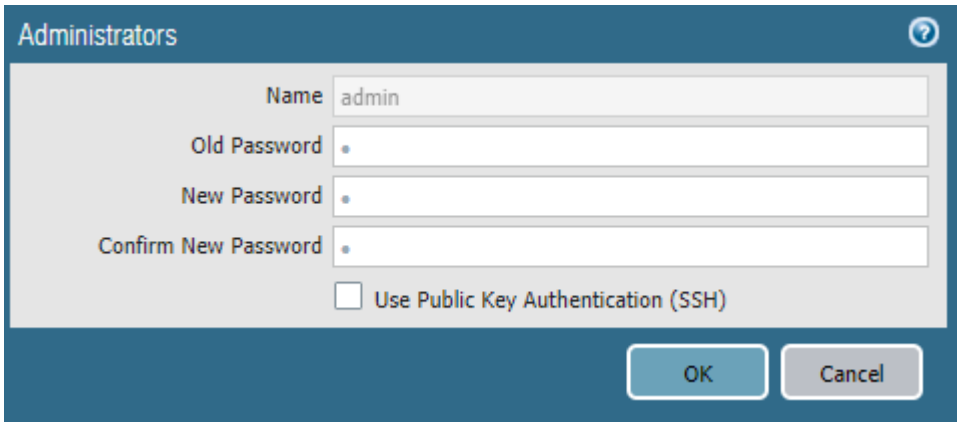


- Kiểm tra: Trong mục tương tự

<u>Đối với tài khoản AAA</u>

- Kiểm tra trực tiếp chính sách trên máy chủ AAA

- Đổi mật khẩu mặc định các tài khoản local của thiết bị
  - Trên GUI:
    - Cấu hình:
      - Chọn mục **Device** > **Administrator** > Click vào **admin** trong cột Name



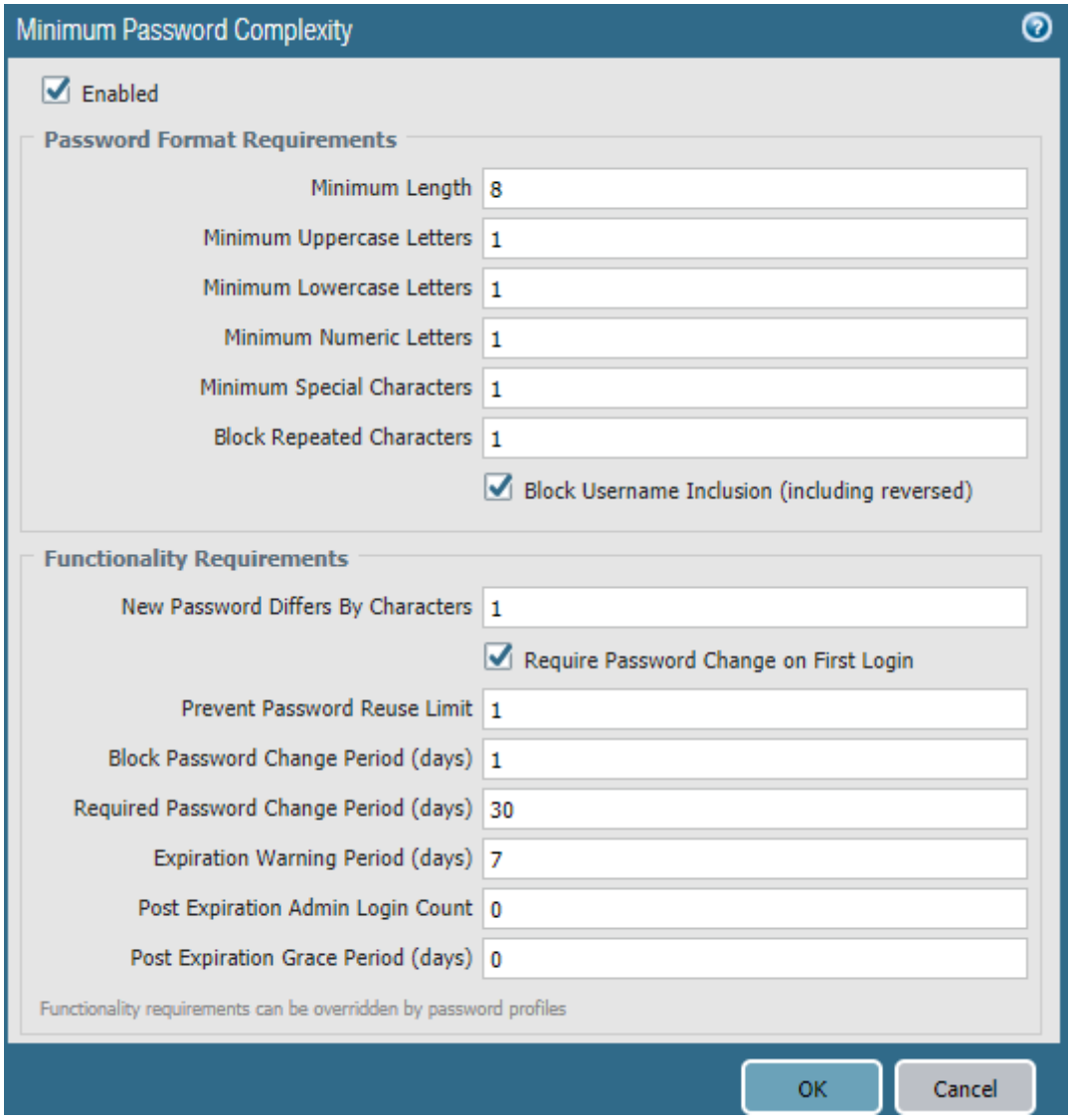
- Đổi mật khẩu mặc định > **OK** > **Click** Commit để apply cấu hình

- Kiểm tra: Trong mục tương tự

- Thiết lập chính sách mật khẩu mạnh cho các tài khoản trên local/AAA. Khóa sau 5 lần đăng nhập sai, thời gian khóa tài khoản do đăng nhập sai là 10 phút

Đối với account local

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Chọn mục Device > Setup > Minimum Password Complexity** > Click vào biểu tượng để edit
    - Tick chọn **Enabled** > Điền các thông số phù hợp > **OK**



- Khóa sau 5 lần đăng nhập sai, thời gian khóa tài khoản do đăng nhập sai là 10 phút: **Đã trình bày ở trên**

- Kiểm tra: Trong mục tương tự

Đối với account AAA

- Kiểm tra trực tiếp chính sách trên máy chủ AAA

4.3. Yêu cầu về kết nối quản trị

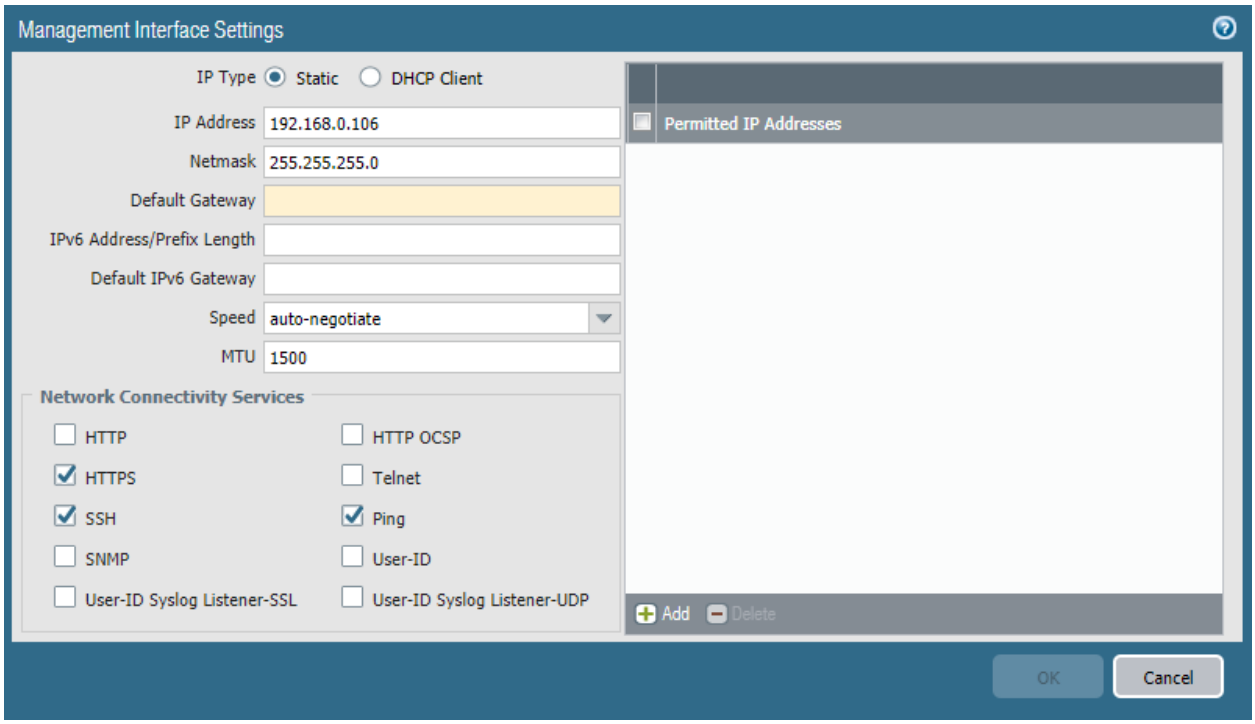
- Quản trị thiết bị qua VLAN quản trị dành riêng.

- Kiểm tra trên cấu hình, đấu nối IP, quy hoạch VLAN quản trị

- Quản trị thiết bị qua kết nối trực tiếp Console hoặc kết nối từ xa an toàn, có mã hóa (SSHv2, HTTPS). Tắt các giao thức quản trị từ xa không an toàn (Telnet, HTTP)

- Cấu hình:

  - Chọn mục **Device > Setup > Interfaces > Management Interfaces Settings**



  - Bỏ tick chọn **Telnet** và **HTTP**

- Giới hạn chỉ cho phép quản trị từ các IP theo danh sách đăng kí

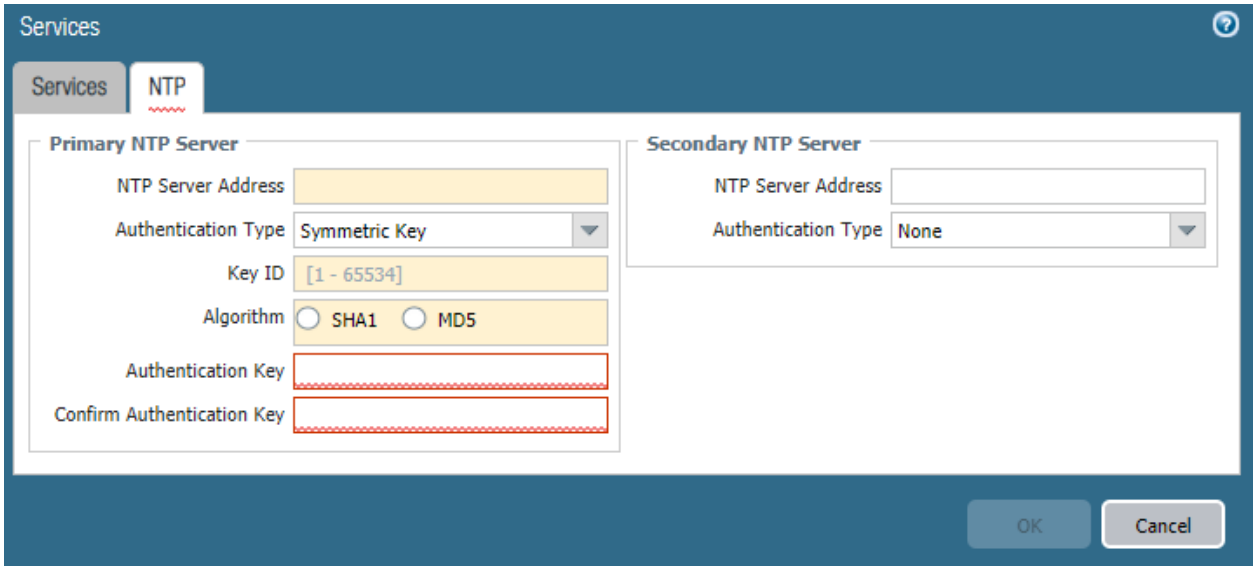
  - Tick chọn **Permitted IP Addresses > Add**
  - Điền IP máy quản trị > Tick chọn IP vừa add > **OK > Click** Commit để apply cấu hình

- Kiểm tra: Trong mục tương tự

4.4. Yêu cầu cấu hình NTP

- Thiết bị phải được đồng bộ thời gian theo tối thiểu 01 máy chủ thời gian (NTP server)

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Device > Setup > Services >** Click vào biểu tượng **> NTP**

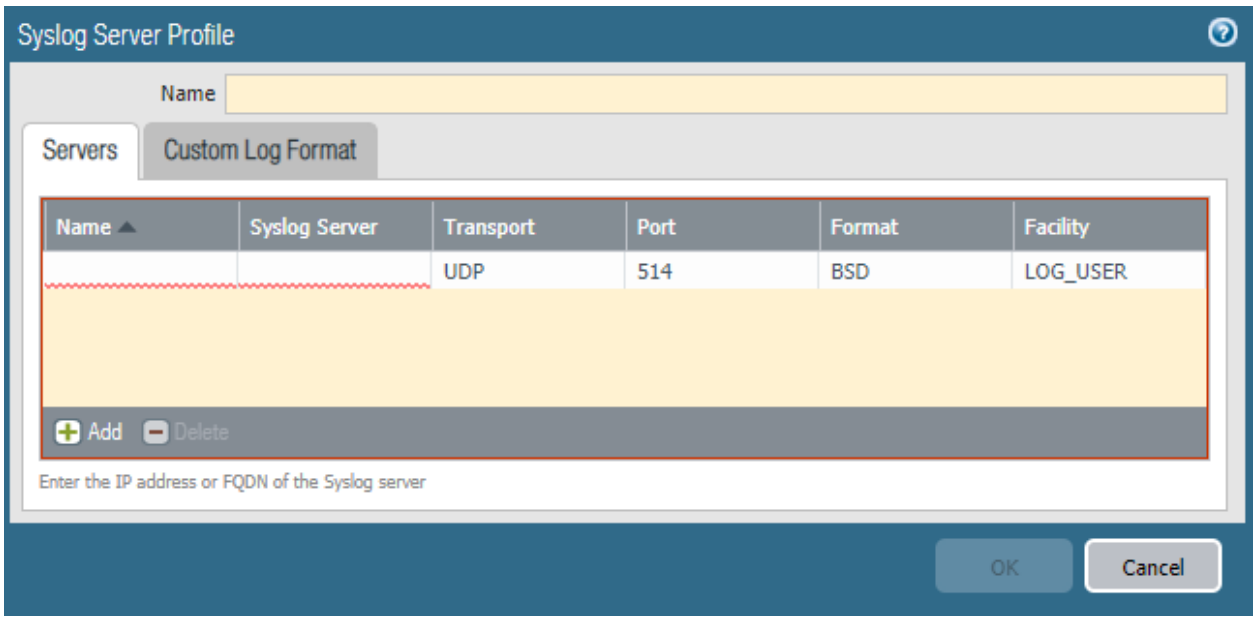


    - Điền IP NTP server, **Authentication type** chọn **Symmetric Key** (optional) > **OK > Click** để apply cấu hình
  - Kiểm tra: Trong mục tương tự

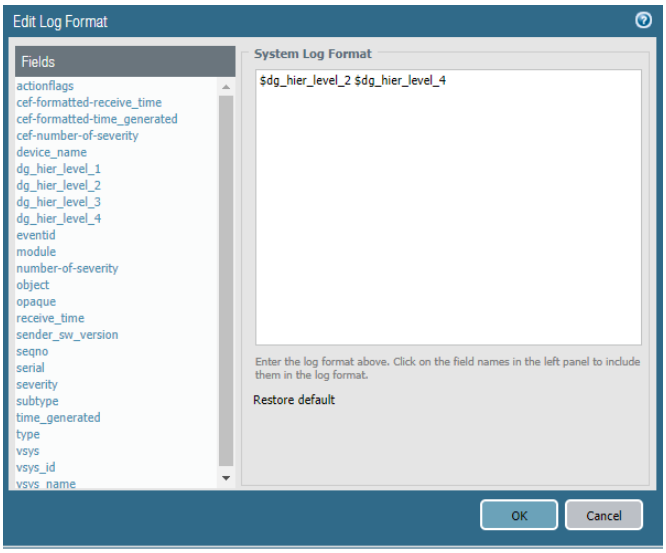
4.5. Yêu cầu cấu hình log

- Thiết bị phải được thiết lập bật chế độ ghi log và cấu hình lưu log tập trung tối thiểu 06 tháng. Trong trường hợp không có hệ thống lưu log tập trung thực hiện thiết lập lưu trên local

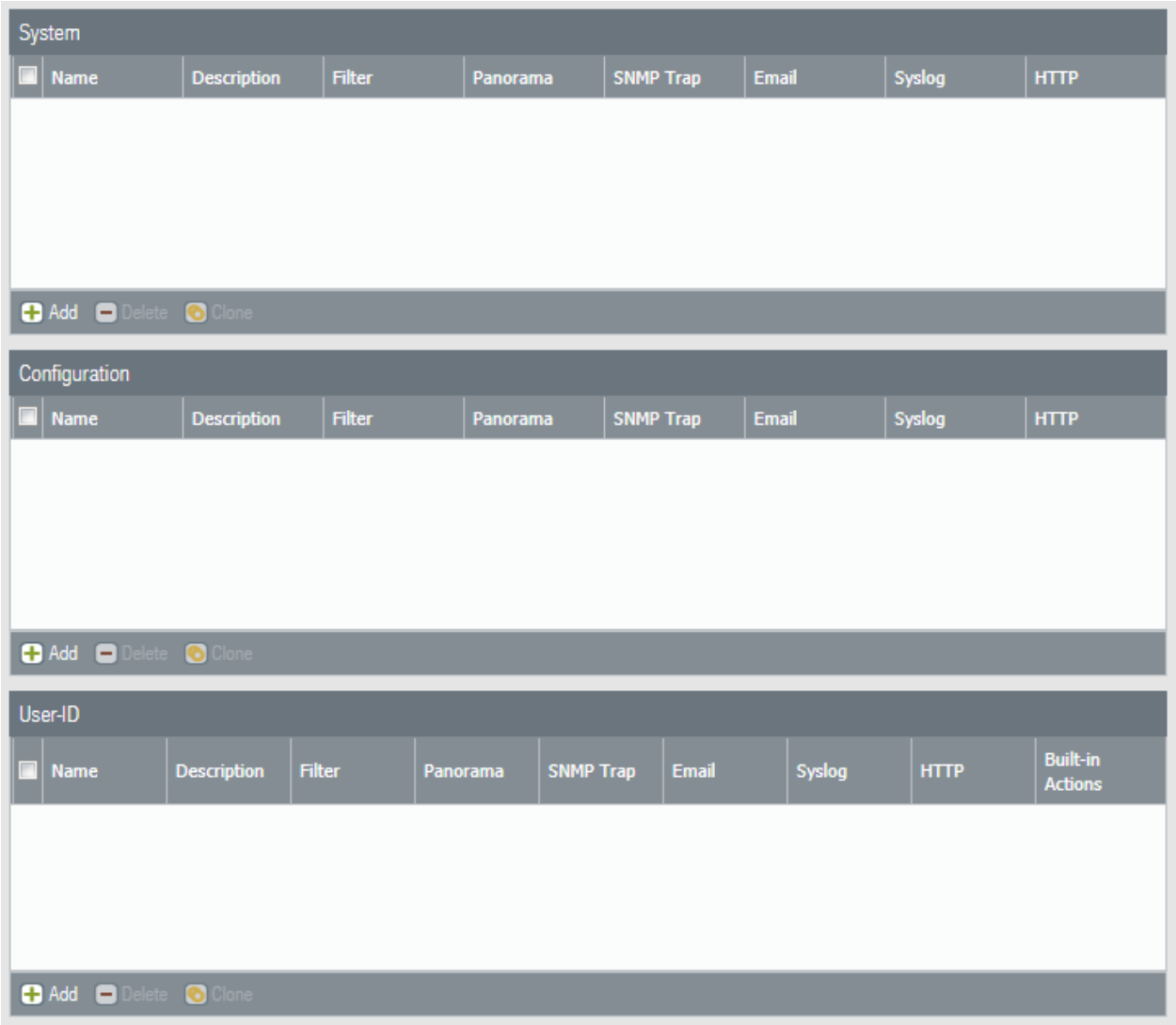
- Trên GUI:
  - Cấu hình:
    - Chọn mục **Device > Server Profiles > Syslog > Add**
    - Điền các thông tin về Syslog svr > **OK**



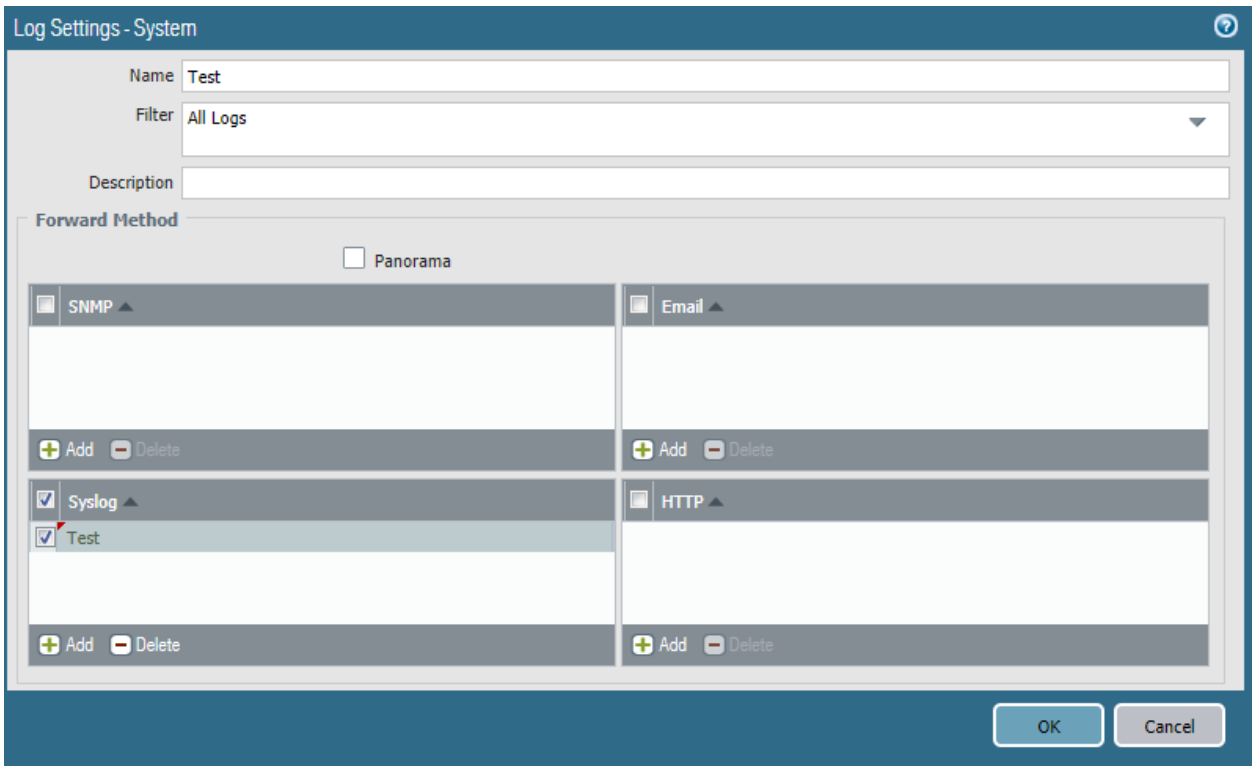
- Có thể chỉnh sửa các trường cho log entry > chọn tab **Custom Log Format (Optional)**



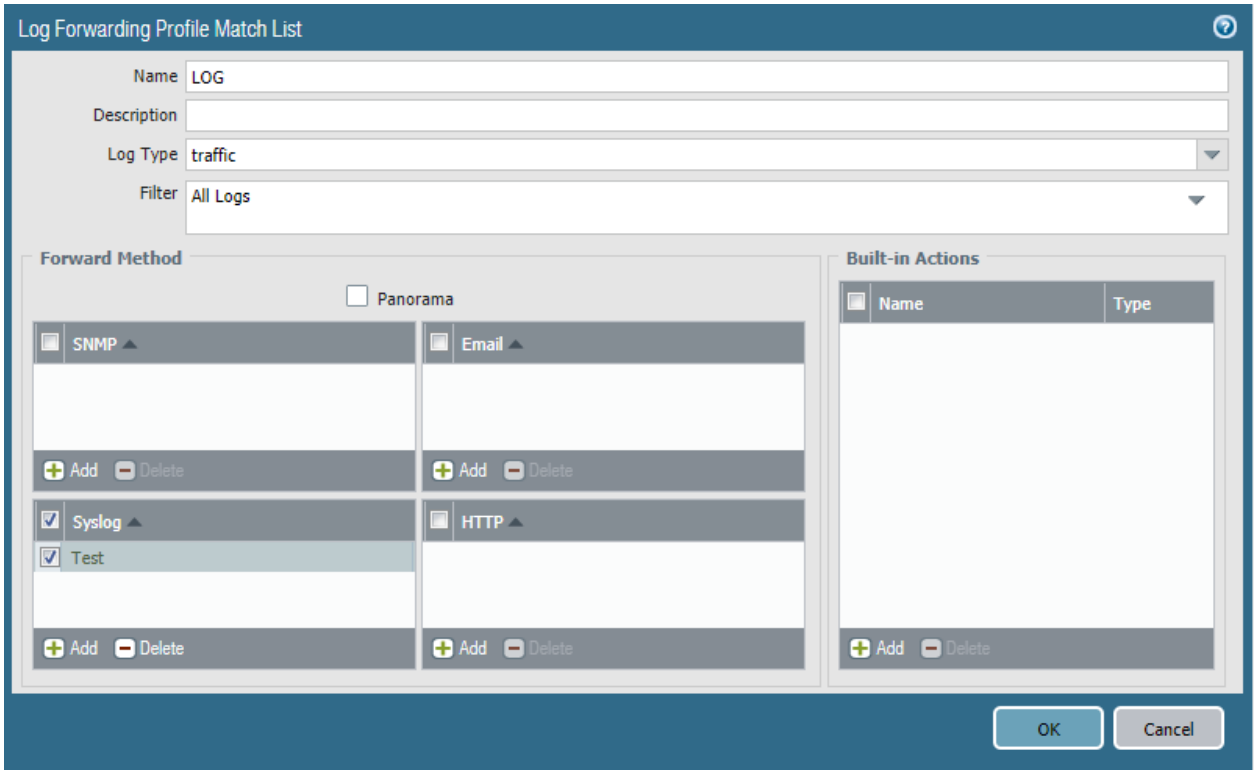
- Chọn mục **Device > Log Settings ()**



- Trong ô loại log muốn lấy > Click **Add**
- **Filter:** Chọn level log muốn lấy **(khuyến nghị lấy log từ Information) >** Trong ô **Forward Method,** tick chọn **Syslog > Add >** chọn profile vừa tạo ở trên > **OK**
- Thực hiện tương tự đối với log Configuration, User-ID…



- Đối với các loại log Traffic, Threat, URL,… chọn mục **Objects >Log Forwarding >** click **Add**



- **Log type:** chọn **Traffic**, **Filter:** chọn **All logs**
- Tick chọn **Syslog**, click **Add**, tick chọn profile đã tạo ở trên > **OK > Click** Commit **để apply cấu hình**

- Đảm bảo trên các policy quan trọng có enable log và log forwarding (mục 5.6)

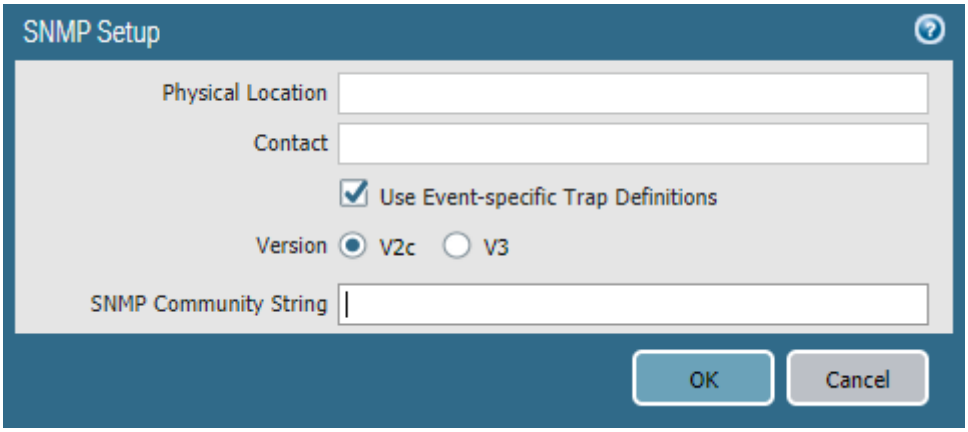
- Kiểm tra: Trong mục tương tự.

4.6. Yêu cầu cấu hình SNMP

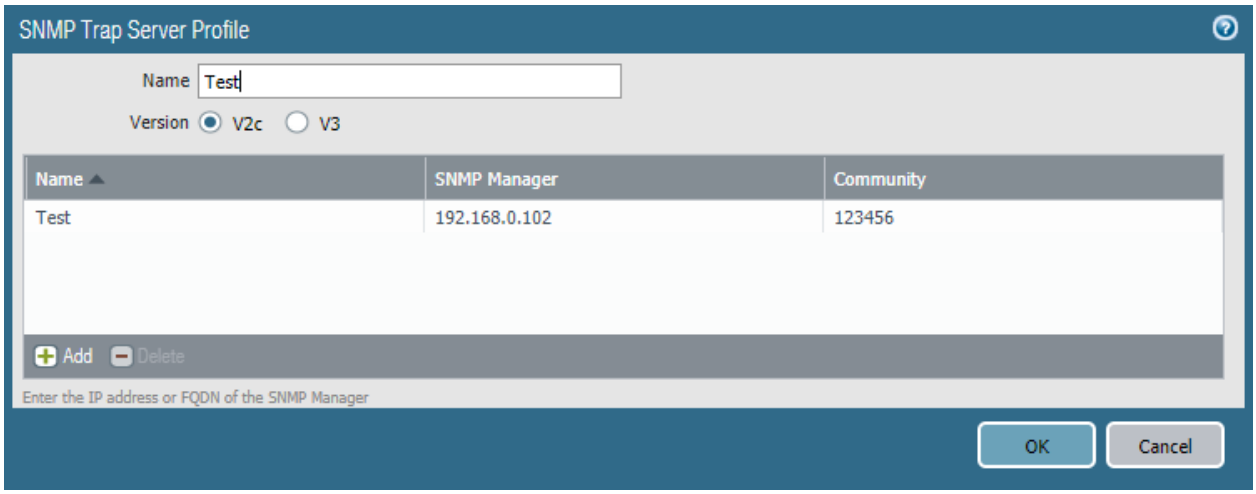
- SNMP phiên bản v2c, v3. SNMP theo chế độ read-only. Community string SNMP riêng. Xóa bỏ community string mặc định. Chỉ cho phép truy cập SNMP từ máy chủ giám sát.

Với SNMP v2c

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Device > Setup > Operations > Miscellaneous > SNMP Setup**
    - Chọn **Version 2c**, khai báo **Community String > OK**



    - Chọn **Device > Server Profiles > SNMP Trap** > Tick chọn **V2c > Add**

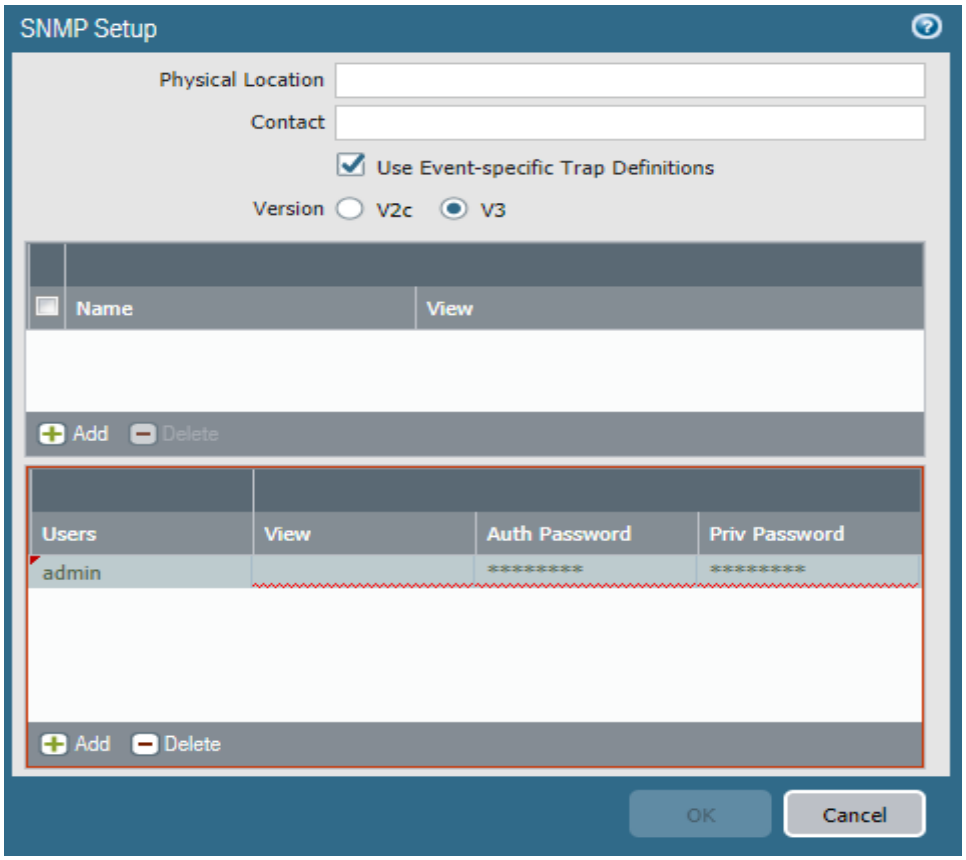


    - Điền các thông tin về Svr SNMP > **OK > Click** Commit để apply cấu hình

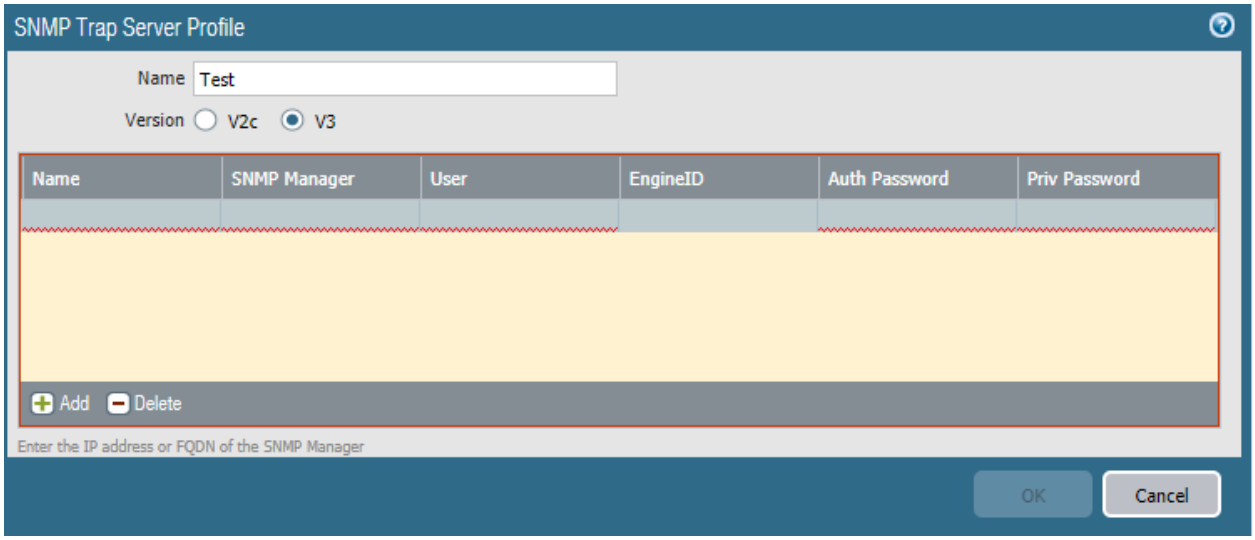
  - Kiểm tra: trong mục tương tự

Với SNMP v3

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Device > Setup > Operations > Miscellaneous > SNMP Setup**
    - Chọn **Version 3**, click **Add**



- Khai báo các thông tin cho SNMPv3 User > **OK**
- Chọn **Device > Sever Profiles > SNMP Trap** > Tick chọn **V3** > **Add**



- Điền các thông tin về Svr SNMP > **OK > Click** Commit để apply cấu hình

- Kiểm tra: trong mục tương tự

5. Thiết lập các tính năng an ninh

5.1. Yêu cầu bật tính năng phòng chống tấn công mạng trên các Firewall

- Bật và cấu hình các tính năng phòng chống tấn công mạng phù hợp với hệ thống CNTT được Firewall bảo vệ (IPS/IDS, UTM, Screening)

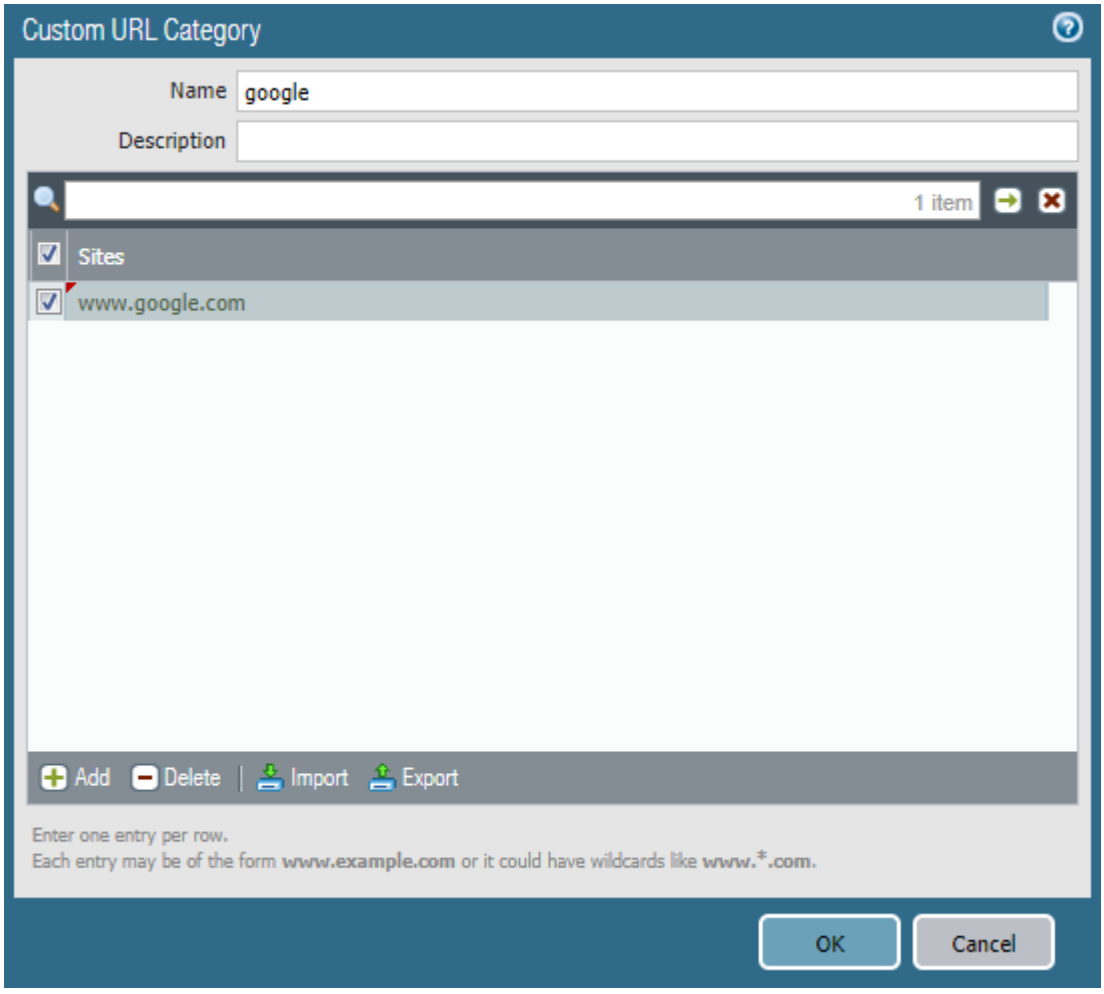
- Firewall Palo Alto thuộc loại Next-Gen Firewall nên các tính năng UTM đã được tích hợp sẵn trên Firewall như URL Filtering, Vulnerability Protection, Anti Virus...

Đối với URL Filtering

- Cấu hình:

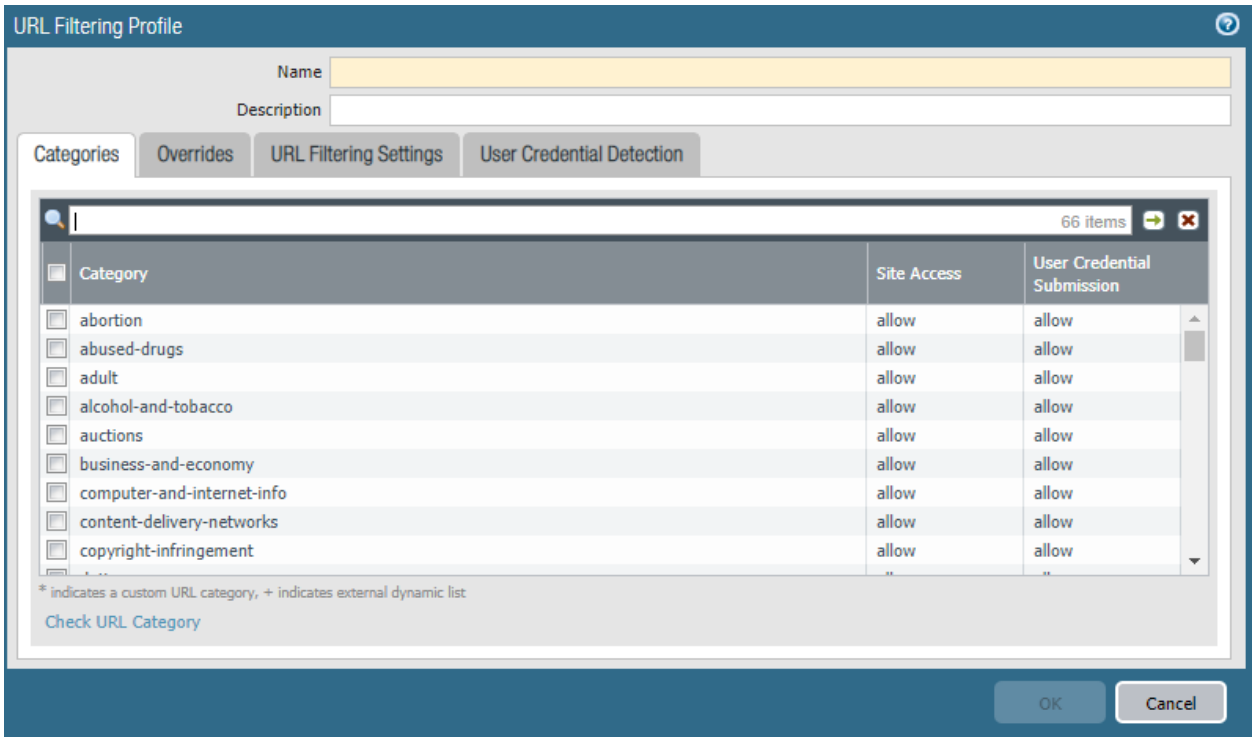
- Tạo URL Categories: Có thể sử dụng Categories của hãng đã define sẵn -> Tham khảo tại link https://urlfiltering.paloaltonetworks.com/

- Chọn mục **Objects > Custom Objects > URL Categories > Add**

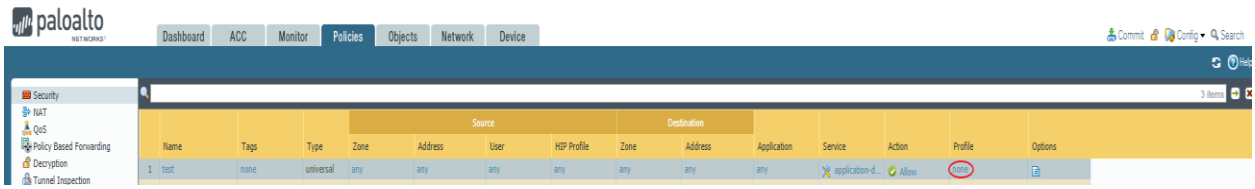


- Click **Add** > điền URL muốn add > **OK**

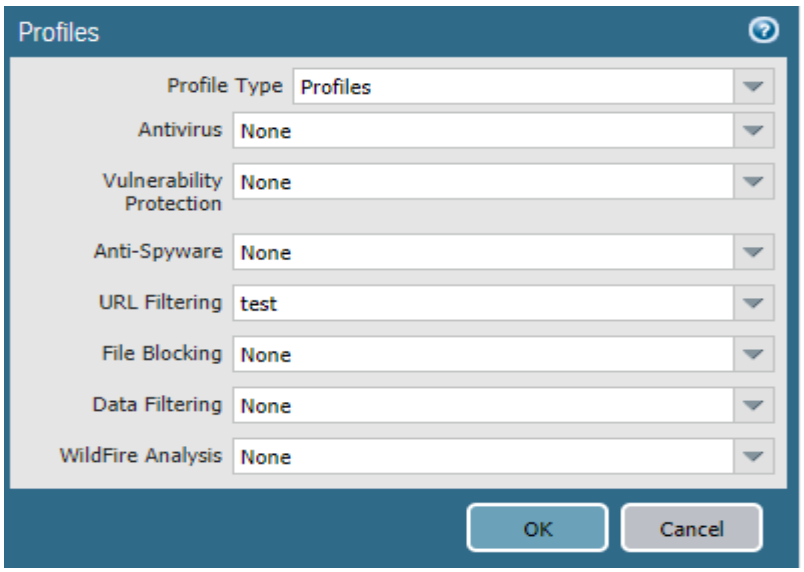
- Tạo URL Filtering Profile
  - Chọn mục **Objects > Security Profiles > URL Filtering** > Click **Add** > tab **Categories.**



  - Tick chọn Categories vừa tạo, có thể chọn thêm các categories của hãng > chọn action trong cột **Site Access > OK**
- Gán Profile vào Firewall Policy
  - Chọn mục **Policies > Security** > chọn policy cần URL-filtering > chọn cột Profile



  - **Profile Type:** chọn **Profiles**
  - **URL-Filtering:** chọn Profile vừa tạo > **OK**



- > **Click** Commit để apply cấu hình

- Kiểm tra: Trong mục tương tự.

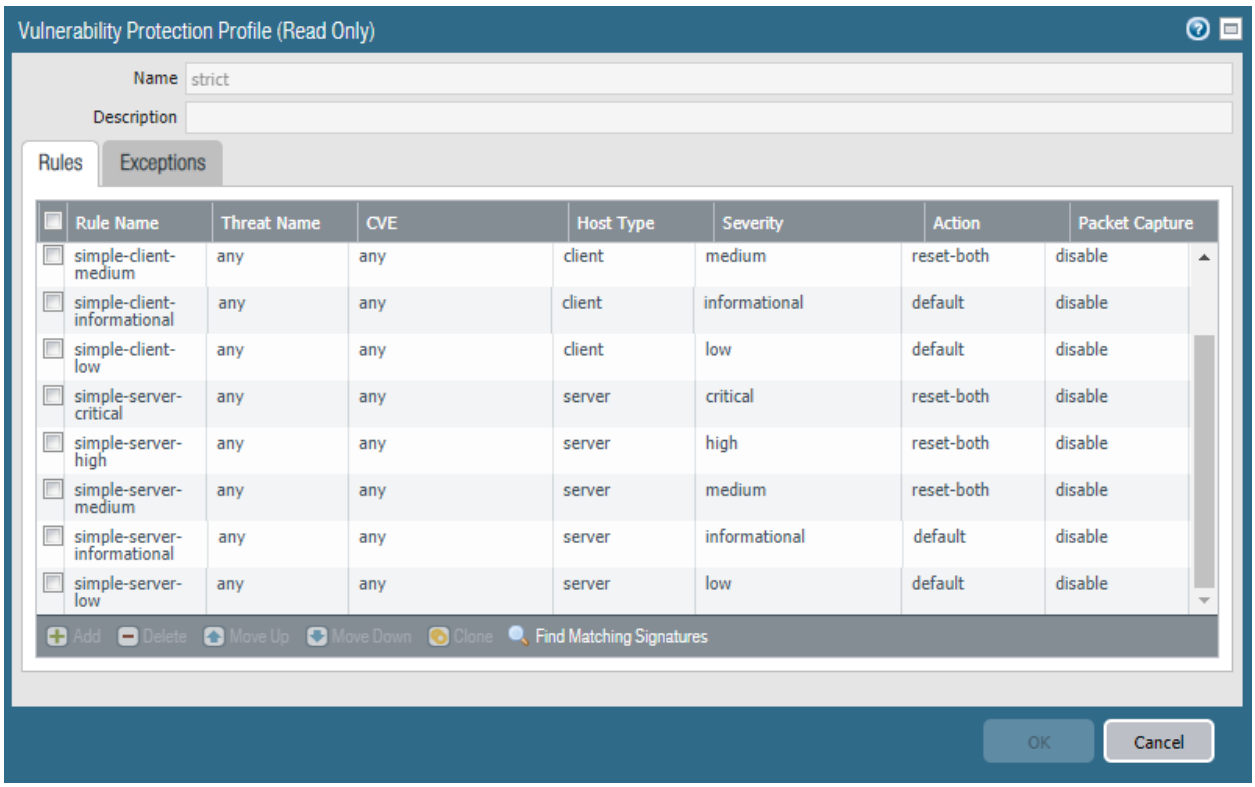
<u>Đối với Vulnerability Protection</u>

- Cấu hình:
  - Palo Alto có sẵn 2 predefined profiles là **strict** và **default** chứa các signatures, rule cùng action tương ứng. Khuyến nghị sử dụng profile **Strict** cho các policy quan trọng (cần theo dõi performance của thiết bị).

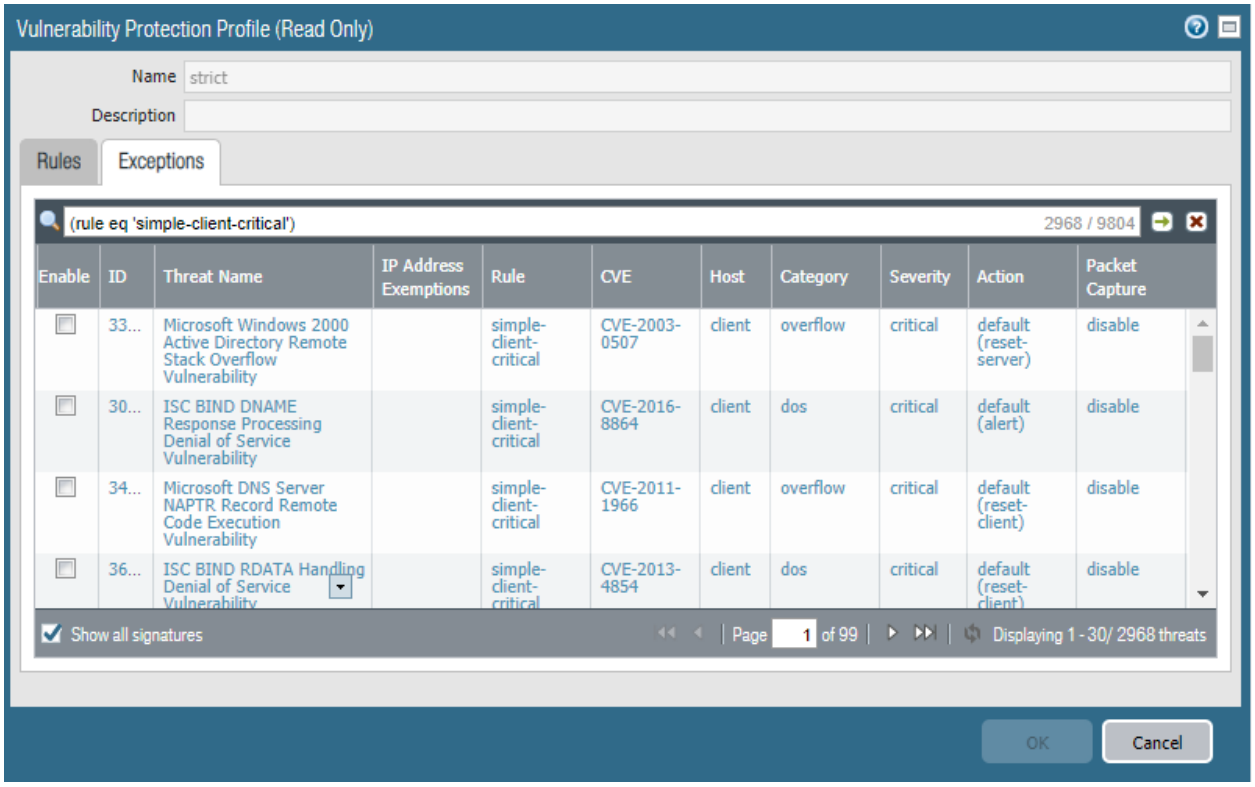
    Strict: Thực hiện block cả phía client và svr (reset-both) đối với những lỗ hổng từ mức medium trở lên. Từ mức low trở xuống sẽ thực hiện action default (được định nghĩa tương ứng với từng signature)

    Default: Thực hiện action default đối với các lỗ hổng mức medium trở lên. Không detect các lỗ hổng mức low trở xuống.

  - Kiểm tra thông tin về profile (signatures, rule, action, severity...)
    - Chọn mục **Objects > Security Profiles > Vulnerability Protection** > Click chọn Profile cần check

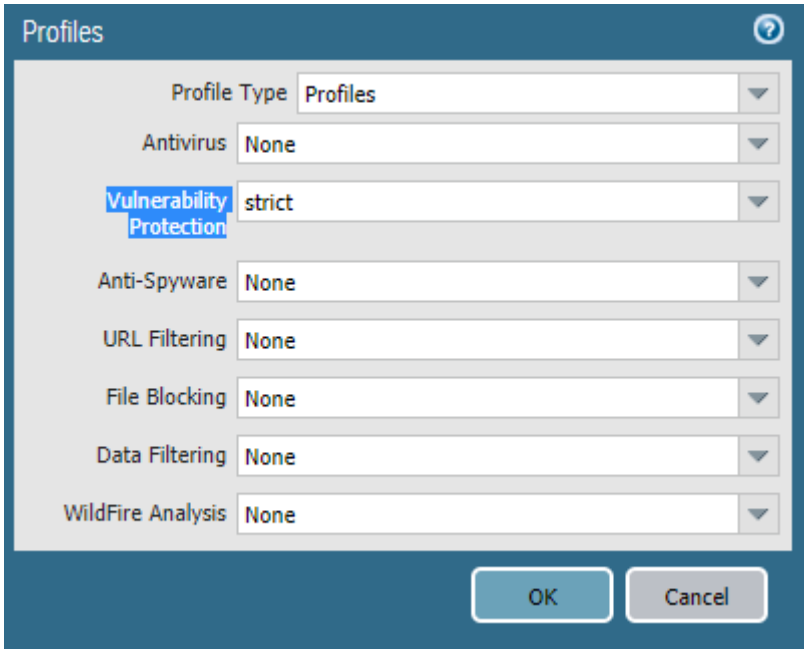


- Tick chọn vào Rule cần check > **Find Matching Signatures**



- Tạo Profile theo ý muốn:
  - Chọn mục **Objects > Custom Objects > Vulnerability > Add**
- Add Profile vào Policy Firewall

- Tương tự với URL-Filtering. Trong trường **Vulnerability Protection** chọn Profile thích hợp > **OK**



- > **Click** Commit để apply cấu hình

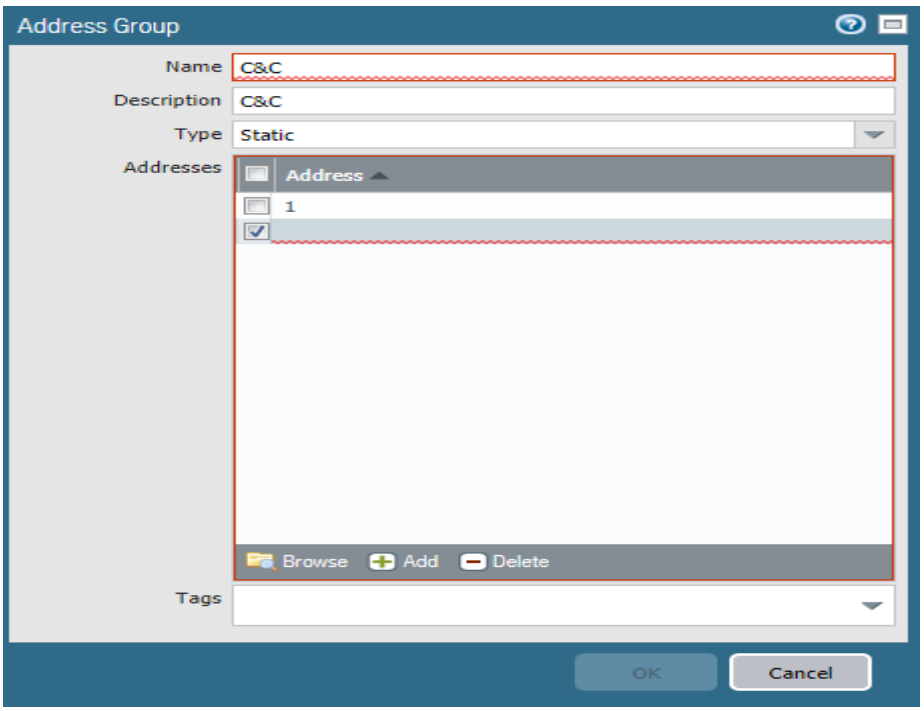
  - Kiểm tra: Trong mục tương tự.

5.2. Yêu cầu rule phát hiện và ngăn chặn các kết nối C&C

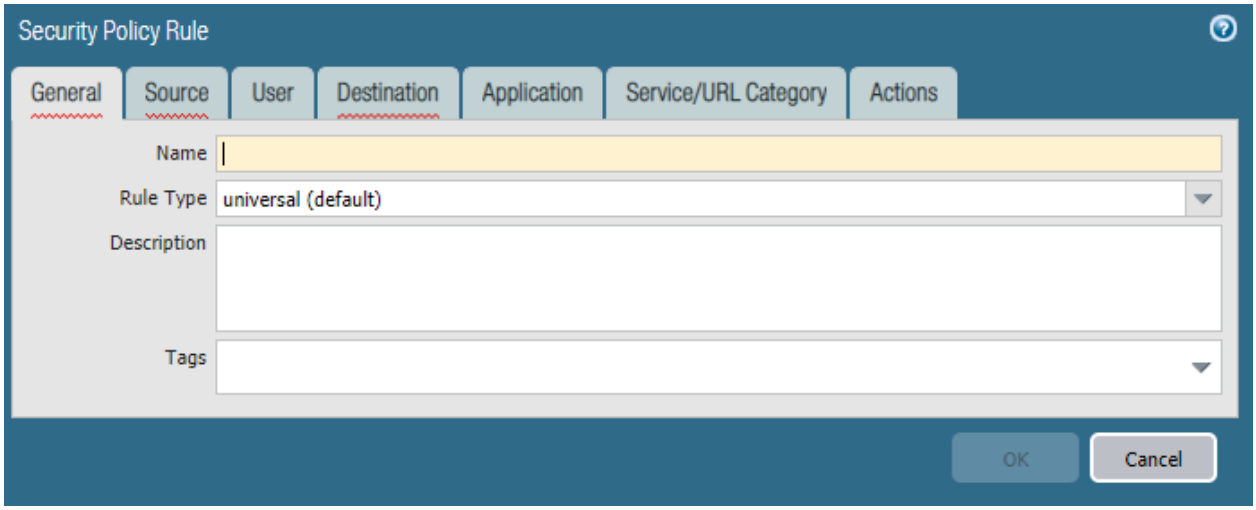
- Khai báo phát hiện và ngăn chặn các kết nối C&C, các domain độc hại. Khai báo rule ở vị trí có hiệu lực đầu tiên

  - Cấu hình

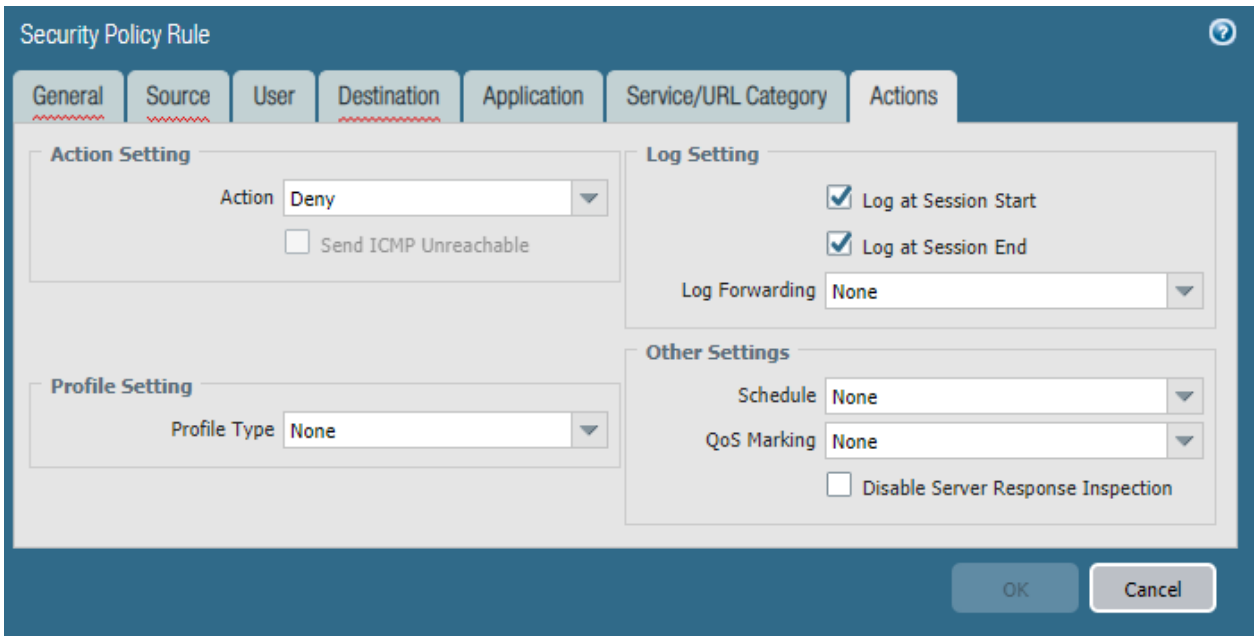
    - Chọn mục **Objects > Address Groups > Add**
    - Tick chọn các IP C&C đã khai báo > **OK**



- Chọn mục **Policies > Security > Add**



- **Tab General: Rule Type** chọn **universal**
- **Tab Source: Source Zone** chọn các Trust Zone**, Source Address** chọn **any**.
- **Tab Destination: Destination Zone** chọn các **Untrust Zone, Destination Address** chọn **Group C&C** vừa tạo.
- **Tab Application** và **Service** chọn **any**
- **Tab Action:** chọn **Deny,** tick chọn **Log at Session Start > OK > Click** Commit để apply cấu hình

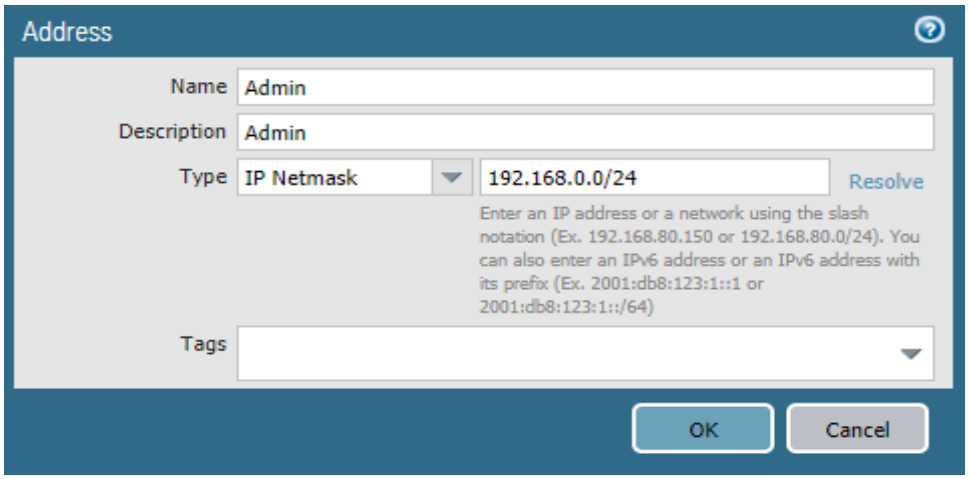


- Kiểm tra: Trong mục tương tự

5.3. Yêu cầu rule phát hiện và chặn người dùng quản trị ra Internet

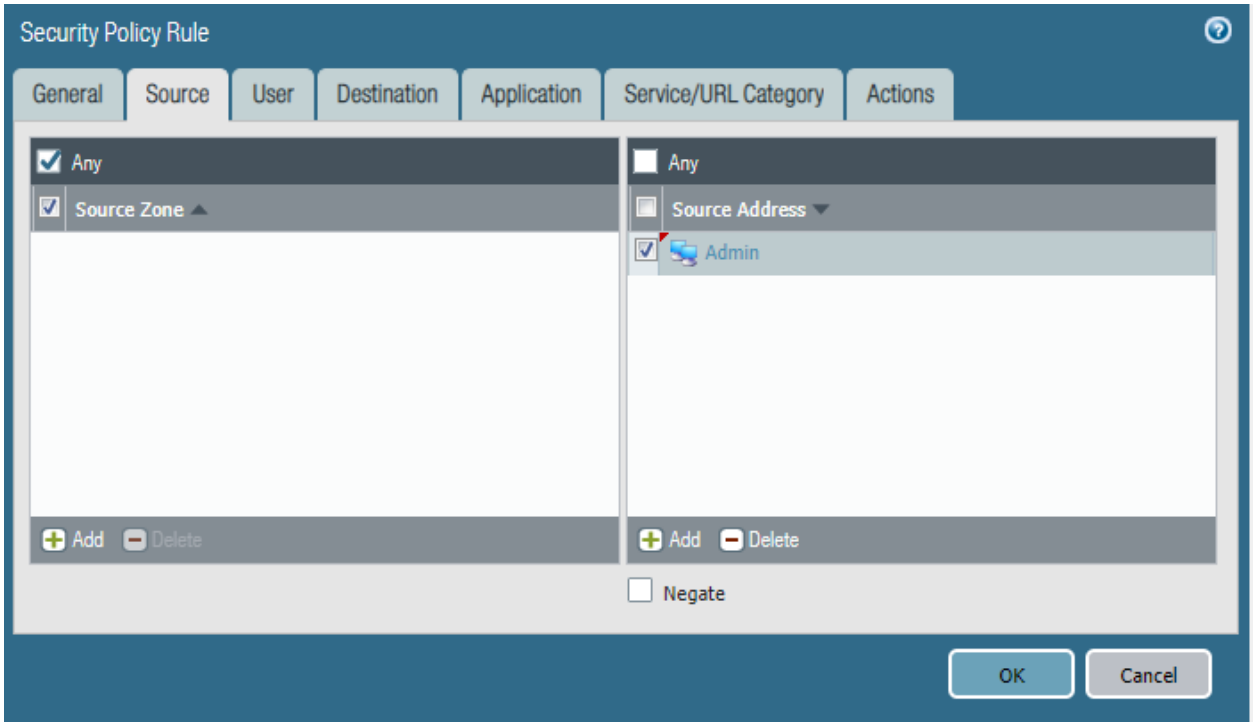
- Khai báo rule phát hiện và chặn người dùng quản trị ra Internet trực tiếp và qua Proxy, chỉ mở cho người dùng quản trị đến các hệ thống theo các port quản trị TCP-22 (SSH), (TCP-23 (Telnet), TCP-3389 (RDP),1433 (MS-SQL), TCP-1521->1527 (Oracle), TCP-3306 (Mysql), TCP-5432 (postgresql), TCP/UDP-161/162 (SMTP)

- Cấu hình
  - Tạo Address dải quản trị
    - Chọn mục **Objects > Address > Add**



    - Điền dải IP quản trị > **OK**
  - Khai báo Policy
    - Chọn mục **Policies > Security > Add**
    - **Tab General: Rule Type** chọn **universal**

- **Tab Source: Source Zone** chọn các TrustZone**, Source Address** chọn **Address Admin** vừa tạo.



- **Tab Destination: Destination Zone** chọn các **Untrust Zone, Destination Address** chọn **any**.
- **Tab Application** và **Service** chọn **any**
- **Tab Action:** chọn **Deny,** tick chọn **Log at Session Start > OK > Click** Commit để apply cấu hình

  - Kiểm tra: Trong mục tương tự

5.4. Yêu cầu rule phát hiện và chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao

- Khai báo rule phát hiện và chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao:

  - Internet: Level 1
  - Wan: Level 2
  - Office: Level 3
  - DMZ: Level 4
  - Server Farm: Level 5
  - Cấu hình
    - Palo Alto có rule mặc định interzone-default chặn kết nối giữa các zone với nhau.

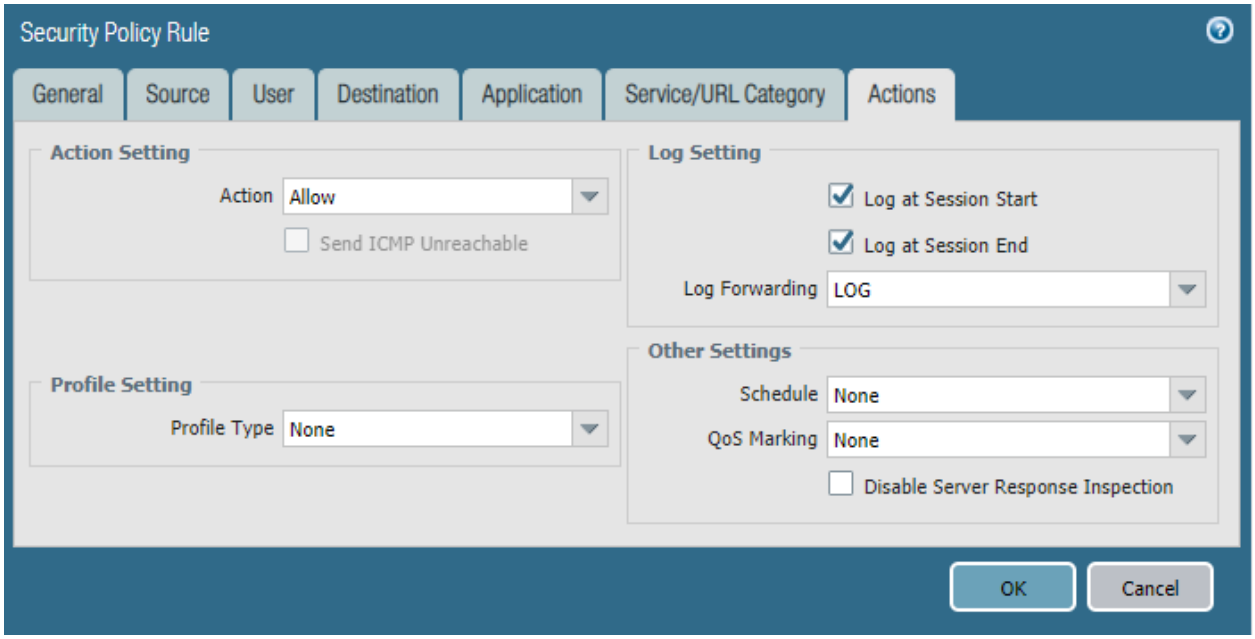
5.5. Yêu cầu rule khai báo Policy vừa đủ các địa chỉ nguồn, địa chỉ đích và port dịch vụ

- Với port quản trị:
  - Mở chi tiết và cụ thể theo ip người dùng và hệ thống được cấp phép trên Firewall Office, Firewall WAN
  - Mở theo dải không qua subnet 24 trên Firewall Server Farm, Firewall DMZ
- Với các port khác:
  - Mở không quá subnet 16
  - Mở không quá range 2000 port
- Với kết nối internet:
  - Được phép mở bất kỳ đích đến với kết nối đi internet

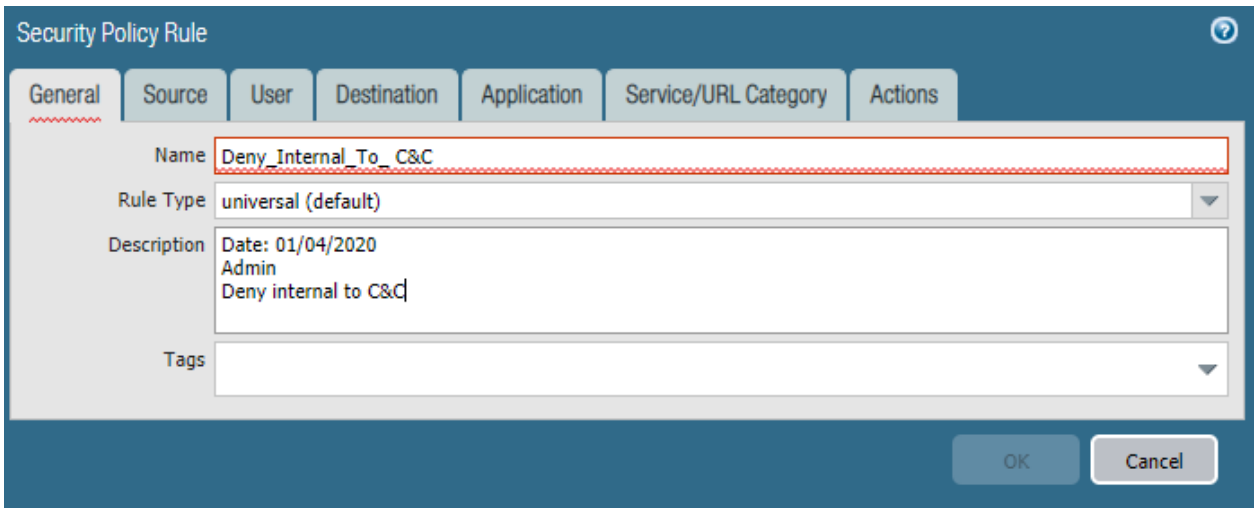
5.6. Yêu cầu rule khai báo phải chứa các thông tin phục vụ kiểm tra và rà soát ATTT

- Khi mở rule cần chú ý mở đúng theo: Title, zone, tags,...

- Các rule quan trọng phải bật lưu logs hoặc bật lưu logs trên tất cả các rule đối với thiết bị nào đang đẩy về hệ thống phân tích logs tập trung



- Các rule cần phải có comment rõ ràng: ngày/tháng/năm mở rule - tên quản trị - rule mở cho mục đích gì - rule mở tạm thời thì cần có thời hạn cụ thể.



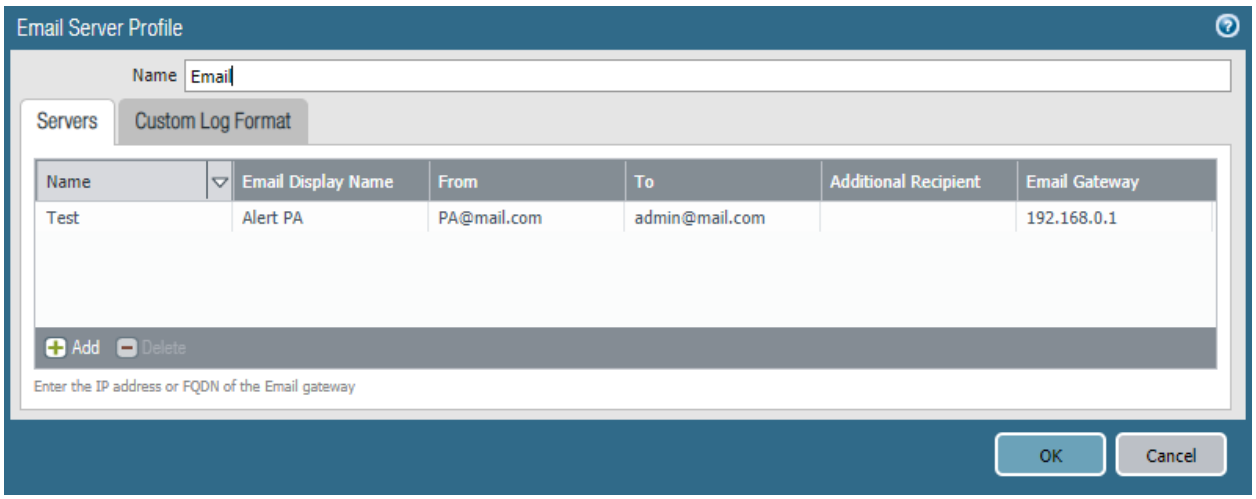
5.7. Yêu cầu IPS/IDS phải update bộ rule mới nhất và đầy đủ

- IPS/IDS phải update bộ rule mới nhất và đầy đủ được ban hành trên website và hệ thống cập nhật của hãng

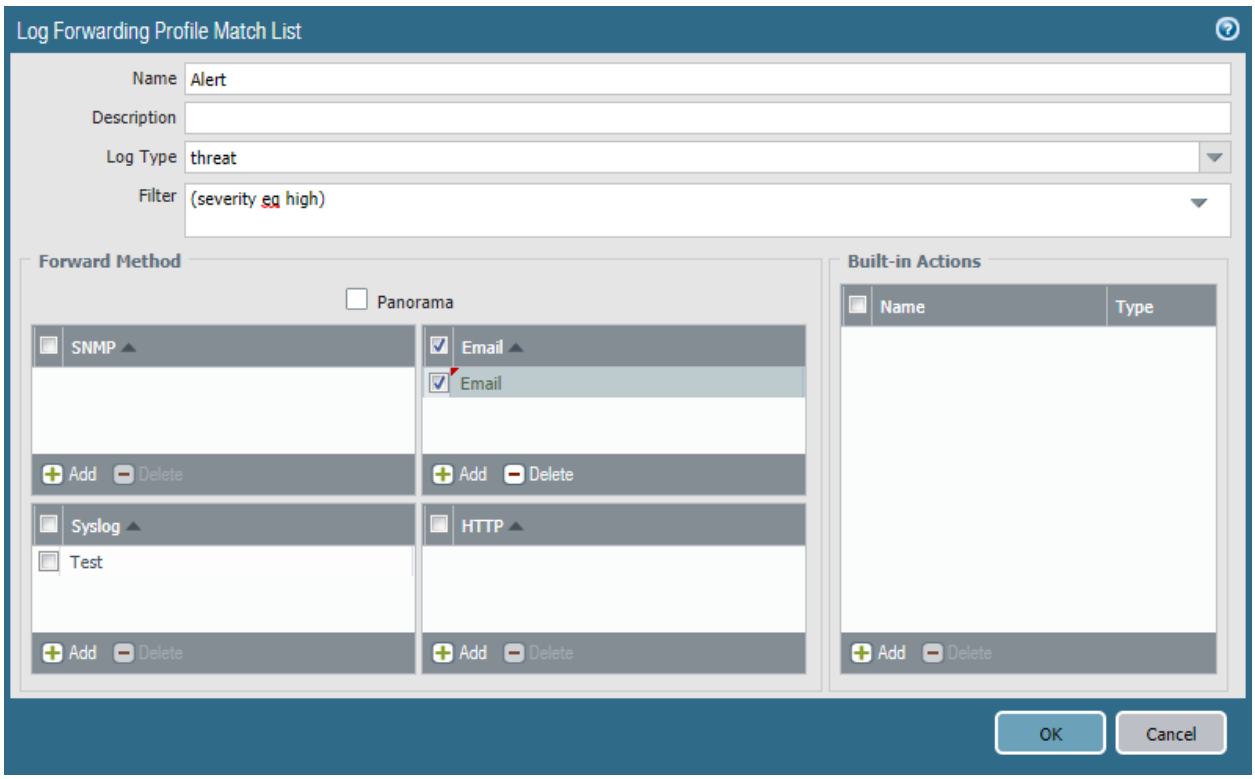
5.8. Yêu cầu thiết lập gửi mail cảnh báo

- Thiết lập gửi mail cảnh báo về người quản trị khi có hành động phát hiện và chặn xâm nhập.

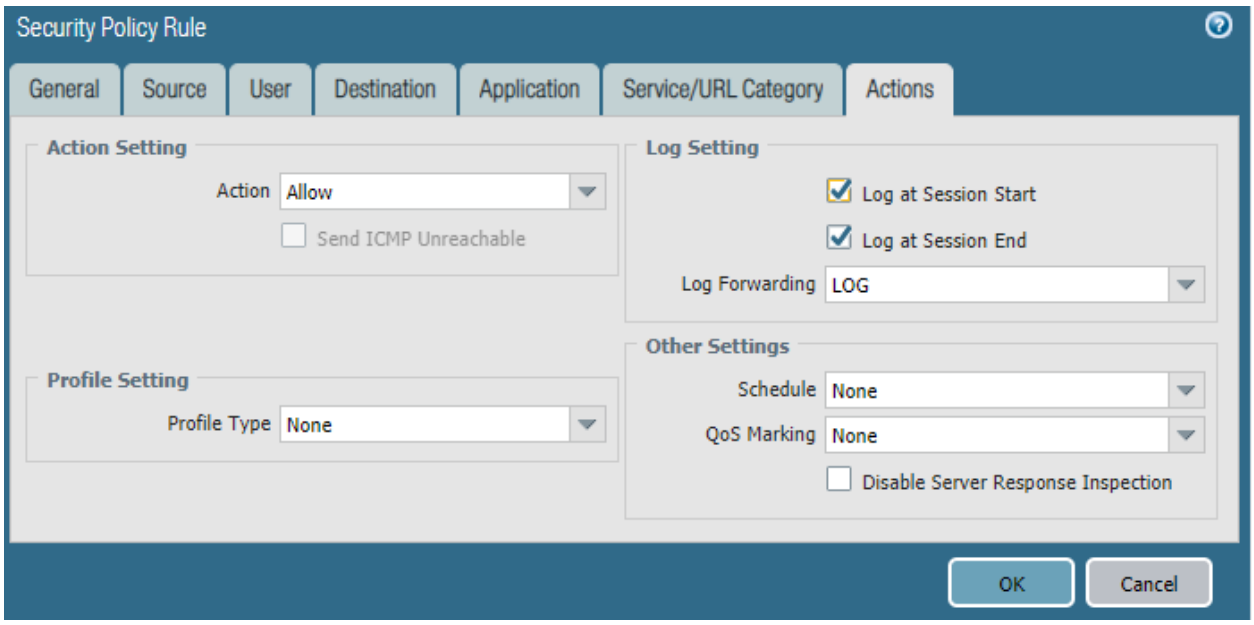
- Trên GUI:
  - Cấu hình
    - Chọn mục **Device > Server Profiles > Email > Add**
    - Điền các thông tin về Email server > **OK**



    - Chọn mục **Objects > Log Forwarding** > Click **add**



- Trong ô **Email** click **Add** để tạo mới hoặc chọn 1 profile có sẵn, tick chọn email profile vừa tạo > **Filter:** chọn **severity eq critical hoặc high > Log type: chọn Threat > OK**
- Chọn mục **Policies** > **Security** > Chọn policy cần gửi cảnh báo > **tab Action** > Tick chọn **Log at...** > **Log Forwarding** chọn Profile vừa tạo > **OK** > > **Click** Commit để apply cấu hình



- Tương tự có thể cấu hình thêm các Email cảnh báo của các option khác như: Traffic, Wildfire, URL....

II. Hướng dẫn cho firewall JUNIPER SCREENOS

1. Yêu cầu chung

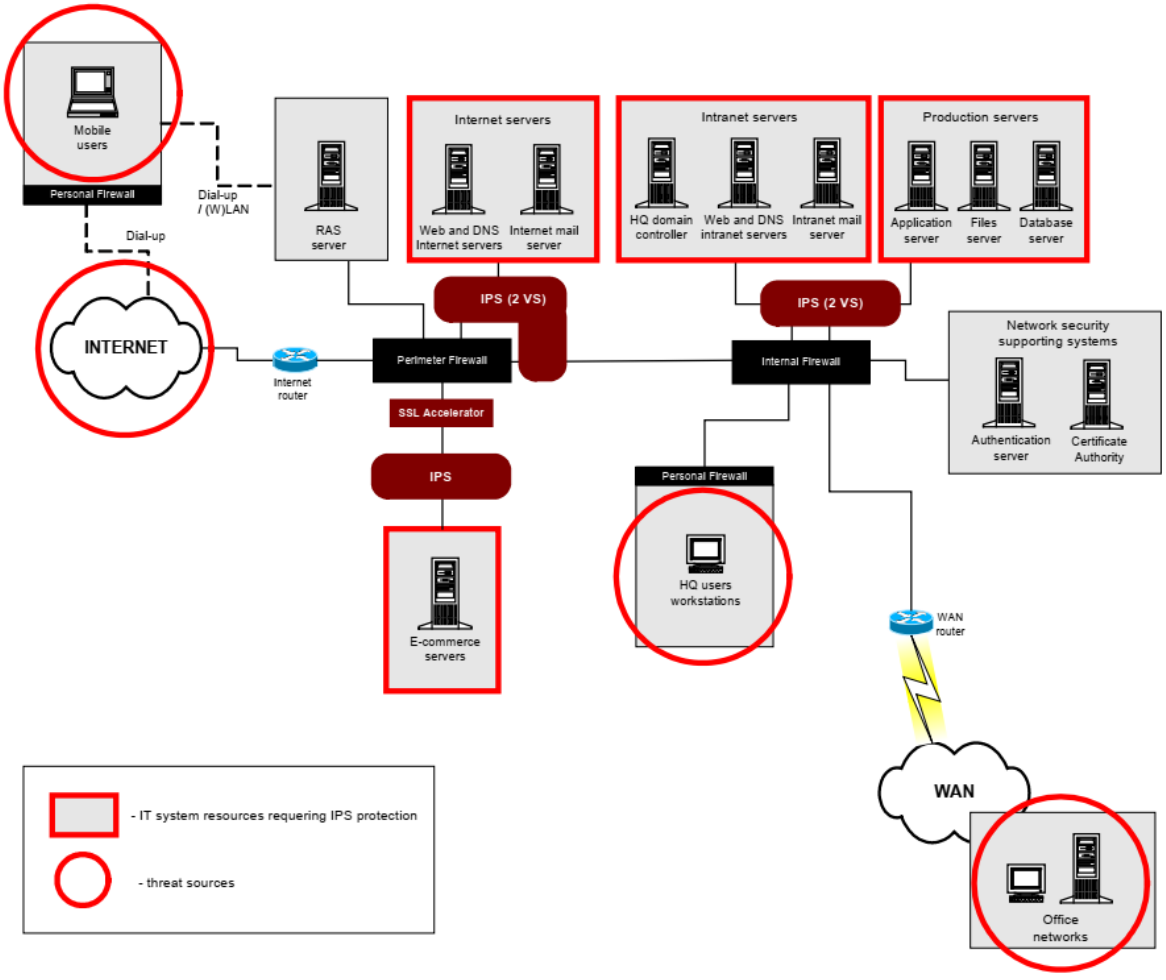
1.1. Yêu cầu phát hiện và chống tấn công từ internet

- Phải đặt IPS/IDS tại các vùng mạng mà monitor được tất cả các traffic in/out internet

  - Đặt tại vùng DMZ kết nối internet
  - Đặt tại vùng người dùng truy cập Internet.

- Phải đặt Firewall giữa kết nối từ Internet vào mạng nội bộ, đảm bảo toàn bộ traffic in/out internet phải đi qua Firewall

  - Đặt tại vùng DMZ kết nối internet
  - Đặt tại vùng người dùng truy cập Internet.



1.2. Yêu cầu phát hiện và chống tấn công từ nội bộ

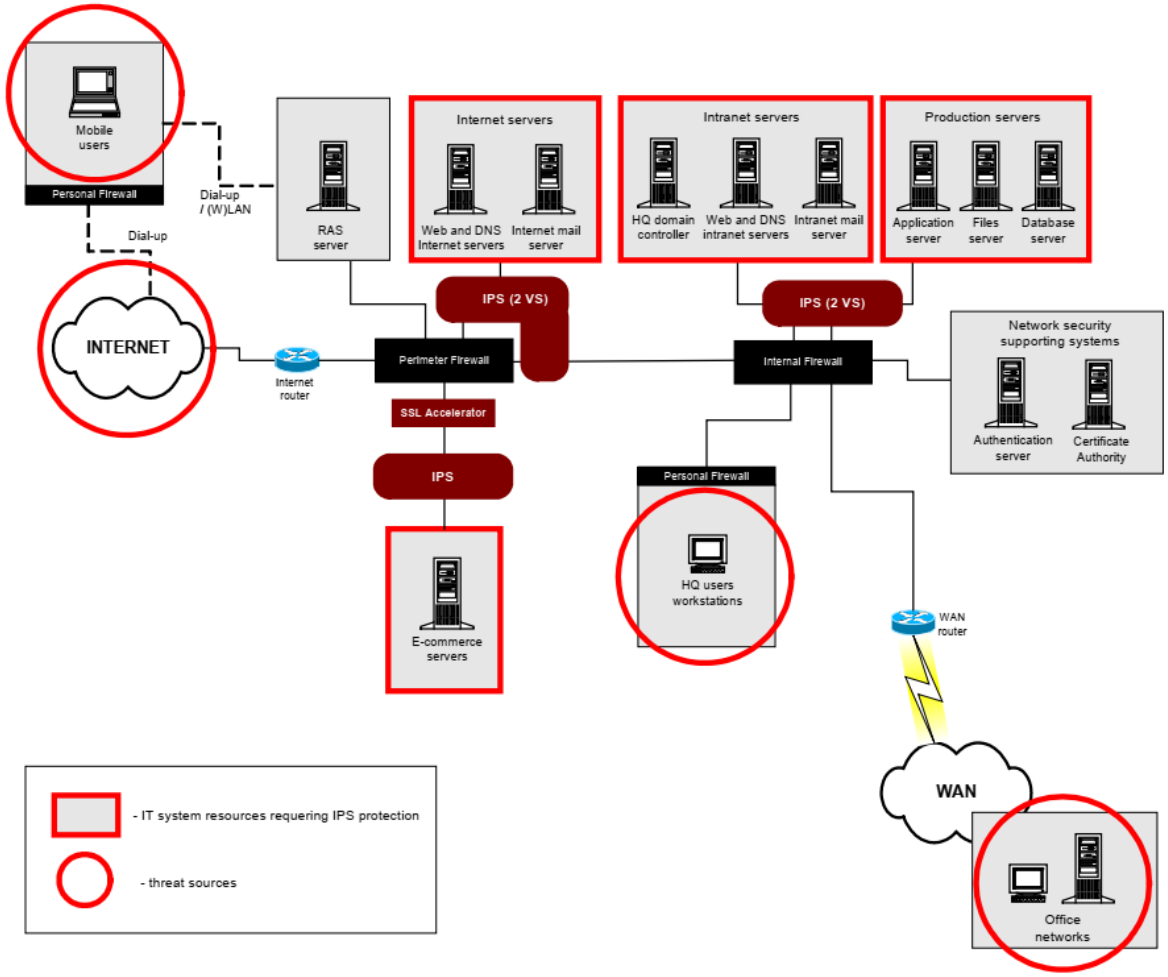
- Phải đặt IPS/IDS tại các vùng mạng mà monitor được tất cả traffice in/out các hệ thống cần bảo vệ

  - Đặt tại vùng Office kết nối vào mạng nội bộ.
  - Đặt tại vùng WAN kết nối vào mạng nội bộ.

- Đặt tại vùng Server Farm kết nối vào mạng nội bộ.
- Đặt tại vùng Partner kết nối vào mạng nội bộ.

- Phải đặt Firewall giữa kết nối từ các hệ thống khác tới hệ thống cần bảo vệ, đảm bảo toàn bộ traffic in/out của vùng mạng cần bảo vệ đi qua Firewall

- Đặt tại vùng Office kết nối vào mạng nội bộ.
- Đặt tại vùng WAN kết nối vào mạng nội bộ.
- Đặt tại vùng Server Farm kết nối vào mạng nội bộ.
- Đặt tại vùng Partner kết nối vào mạng nội bộ.

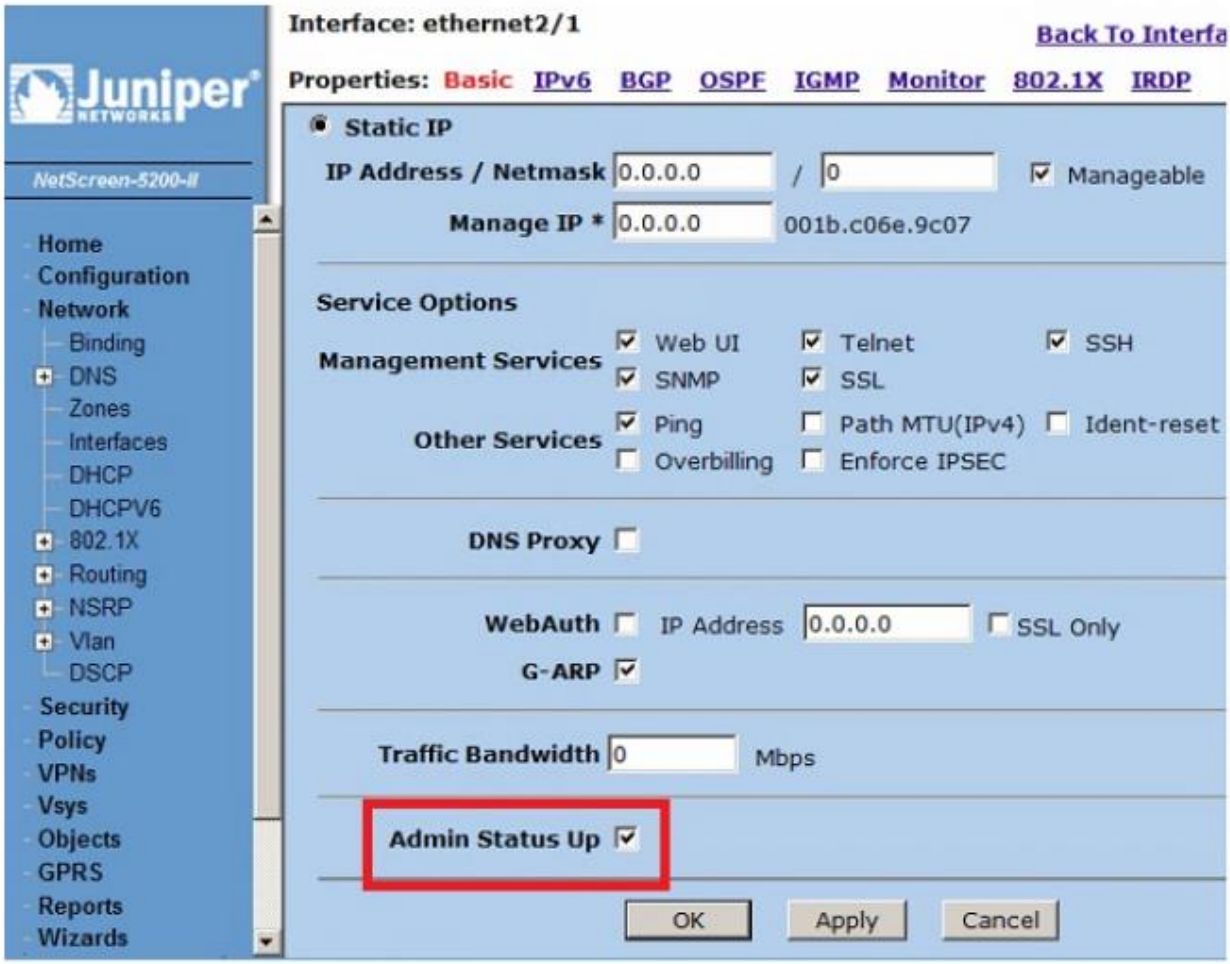


2. Cấu hình an ninh lớp 1

2.1. Yêu cầu shutdown port không sử dụng

- Shutdown tất cả các port không sử dụng trên thiết bị, chỉ bật lên khi có yêu cầu sử dụng

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Network** >**Interfaces** > Chọn interface cần cấu hình
    - Bỏ tick **Admin Status up** để tắt cổng > **Apply**



- Trên CLI:
  - Cấu hình:

```
> edit
Entering configuration mode
[edit]
set interface [interface name] disable
```

  - Kiểm tra: Trong mục tương tự

2.2. Yêu cầu mô tả kết nối rõ ràng

- Cổng đang bật phải có mô tả kết nối rõ ràng xác định được thông tin đấu nối của thiết bị đầu xa

- Trên GUI: Không support
- Trên CLI:

```
> edit
Entering configuration mode
[edit]
```

```
set int [interface name] description [text]
```

- Kiểm tra:

```
SSG520-> get interface [interface name]
```

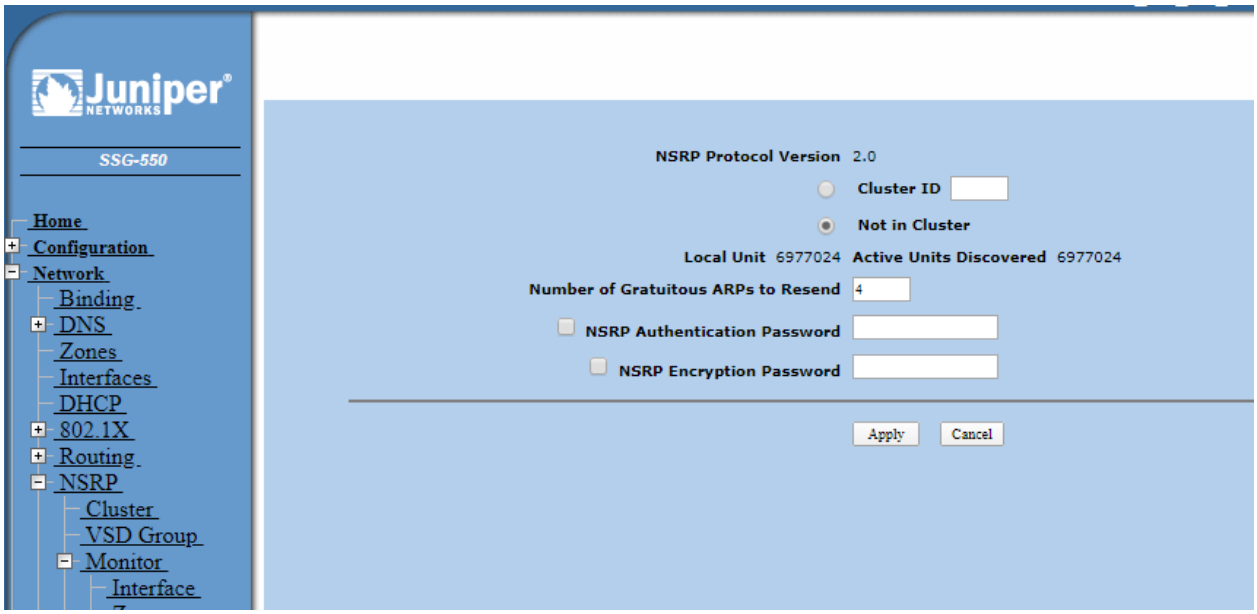
3. Cấu hình an ninh lớp 3

3.1. Xác thực cho các giao thức lớp 3

- VRRP, HSRP, GLBP, NSRP phải cấu hình xác thực cho giao thức giữa các thiết bị

Firewall Juniper SSG550 hỗ trợ giao thức NSRP.

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Network > NSRP > Cluster**
    - Nhập mật khẩu vào ô **NSRP authentication password**



- Trên CLI:

```
> edit
Entering configuration mode
[edit]
set nsrp encrypt password hBsm8xVGdpqusGT
set nsrp auth password cGvVjn5gYUF2yJK
```

- OSPF phải thiết lập chuỗi xác thực có mã hóa giữa 2 thiết bị

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Network > Interface > Edit > OSPF**
    - Trong **Authentication** chọn **MD5 Keys**(Preferred) hoặc **password**(clear text)
    - **Nhập mã và Click Apply**
  - Trên CLI:

```
> edit
Entering configuration mode
[edit]
set interface ethernet1 protocol ospf authentication md5 1234567890123456
set interface ethernet1 protocol ospf authentication md5 9876543210987654 key-id 1
set interface ethernet1 protocol ospf authentication md5 active-md5-key-id 1
Hoặc
set interface ethernet1 protocol ospf authentication password 12345678
save
```

  - Kiểm tra: Trong mục tương tự

- Chuỗi xác thực:
  - Có độ phức tạp bao gồm chữ in thường, in hoa, ký tự
  - Chuỗi dài từ 16 ký tự trở lên (MD5) hoặc 10 ký tự (clear text)
  - Không đặt các mật khẩu dễ đoán
- RIP phải thiết lập chuỗi xác thực có mã hóa giữa 2 thiết bị
  - Trên GUI:
    - Cấu hình:
      - Chọn mục **Network > Interface > Edit > RIP**
      - Trong **Authentication** chọn **MD5 Keys**.
      - N**hập mã vào 2 key field**
      - Trong Key ID: 1 chọn **Preferred**
      - **Click Apply**
  - Trên CLI:

```
> edit
Entering configuration mode
[edit]
set interface ethernet1 protocol rip authentication md5 1234567890123456
```

```
set interface ethernet1 protocol rip authentication md5 9876543210987654 key-id 1
set interface ethernet1 protocol rip authentication md5 active-md5-key-id 1
save
```

- Kiểm tra: Trong mục tương tự

- Chuỗi xác thực:
  - Có độ phức tạp bao gồm chữ in thường, in hoa, ký tự
  - Chuỗi dài từ 16 ký tự trở lên
  - Không đặt các mật khẩu dễ đoán
- BGP phải thiết lập chuỗi xác thực có mã hóa giữa 2 thiết bị
  - Trên GUI:
    - Cấu hình:
      - Chọn mục **Network > Routing > Virtual Router > Edit** (trust-vr) > Chọn Peer cần cấu hình
      - Trong **Peer authentication** nhập mã xác thực
      - **Click OK**
  - Trên CLI:

```
> edit
Entering configuration mode
[edit]
set vrouter trust-vr protocol bgp neighbor peer-group ibgp md5-authentication verify03
save
```

- Kiểm tra: Trong mục tương tự

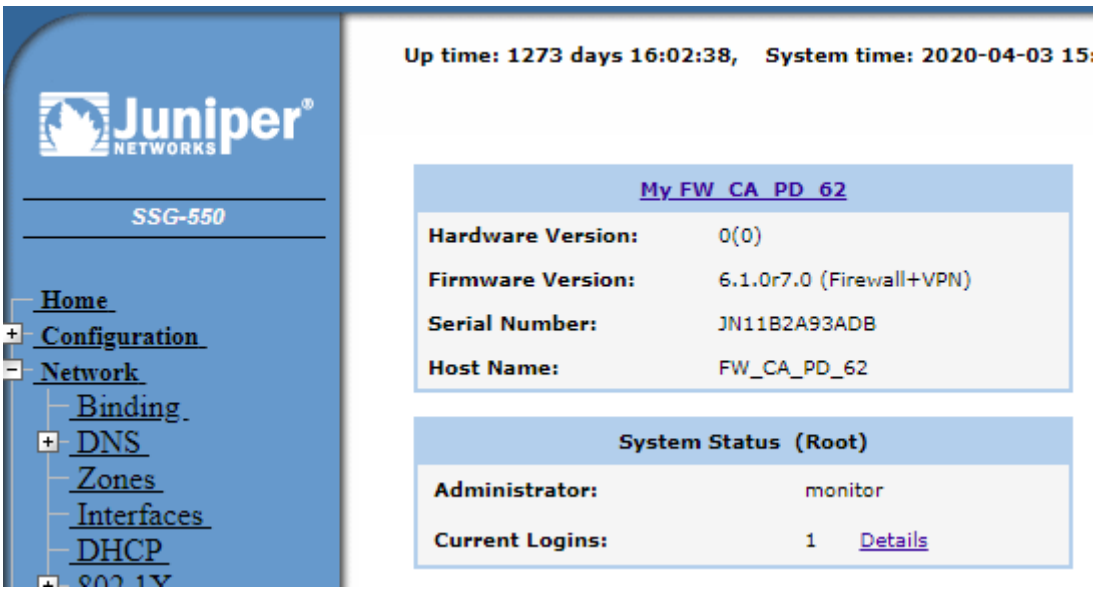
- Chuỗi xác thực:
  - Có độ phức tạp bao gồm chữ in thường, in hoa, ký tự
  - Chuỗi dài từ 16 ký tự trở lên (MD5) hoặc 10 ký tự (clear text)
  - Không đặt các mật khẩu dễ đoán

4. Cấu hình quản trị

4.1. Yêu cầu về sao lưu cấu hình

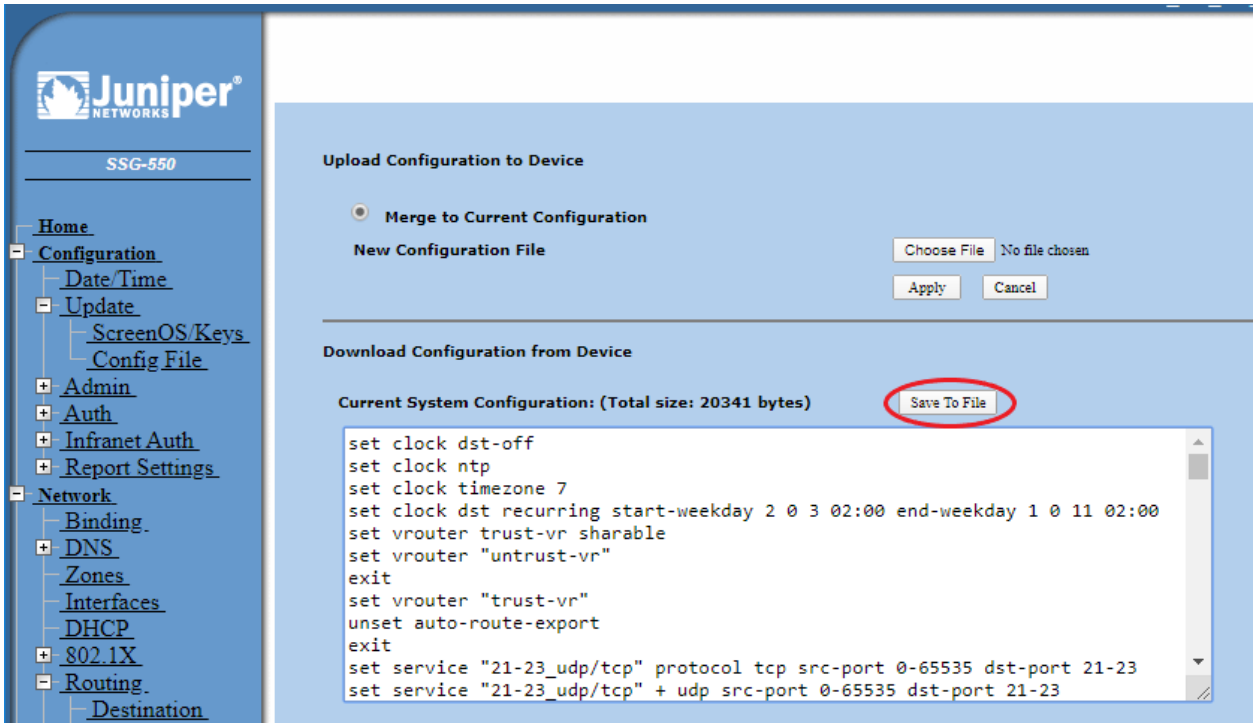
- Thiết bị phải được sử dụng phiên bản hệ điều hành và cập nhật các bản vá đảm bảo an toàn theo yêu cầu của bộ phận ATTT

- Trên GUI:
  - Kiểm tra:
    - Tại màn hình chính **Dashboard**



- Lưu cấu hình trước khi tác động và định kì tối thiểu 01 lần/tuần. Lưu tối thiểu 02 bản gần nhất. Không lưu bản sao lưu trên máy tính cá nhân của quản trị viên.

- Trên GUI:
  - Cấu hình: (Không support đẩy backup config tự động)
    - Lưu cấu hình thủ công: Chọn mục **Configuration** > **Update** > **Config File** > Click **Save to File**



- Trên CLI:

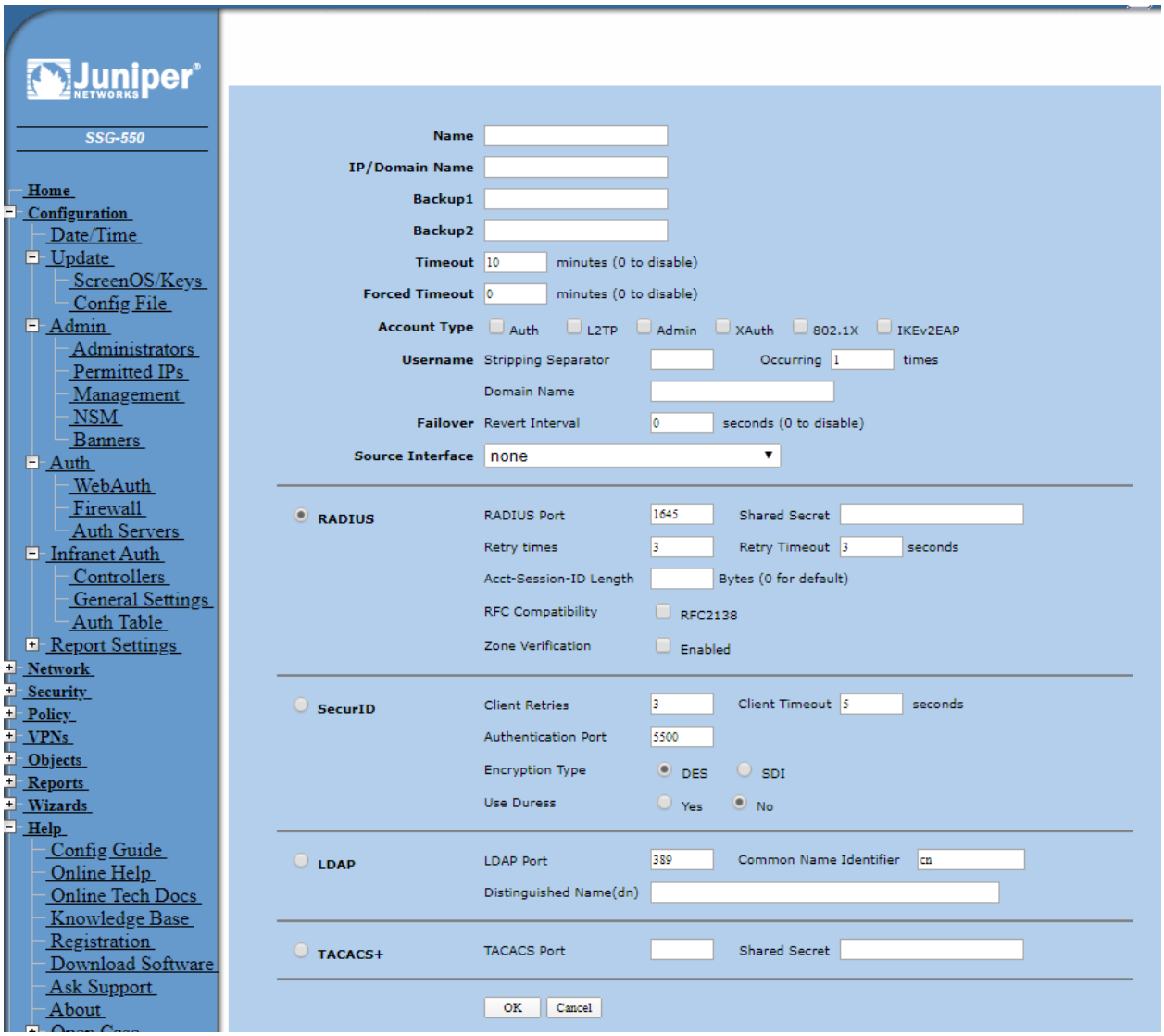
save config to tftp <tftp_server_ip> <config_filename>

- Kiểm tra: Kiểm tra file cấu hình được lưu trên máy tính.

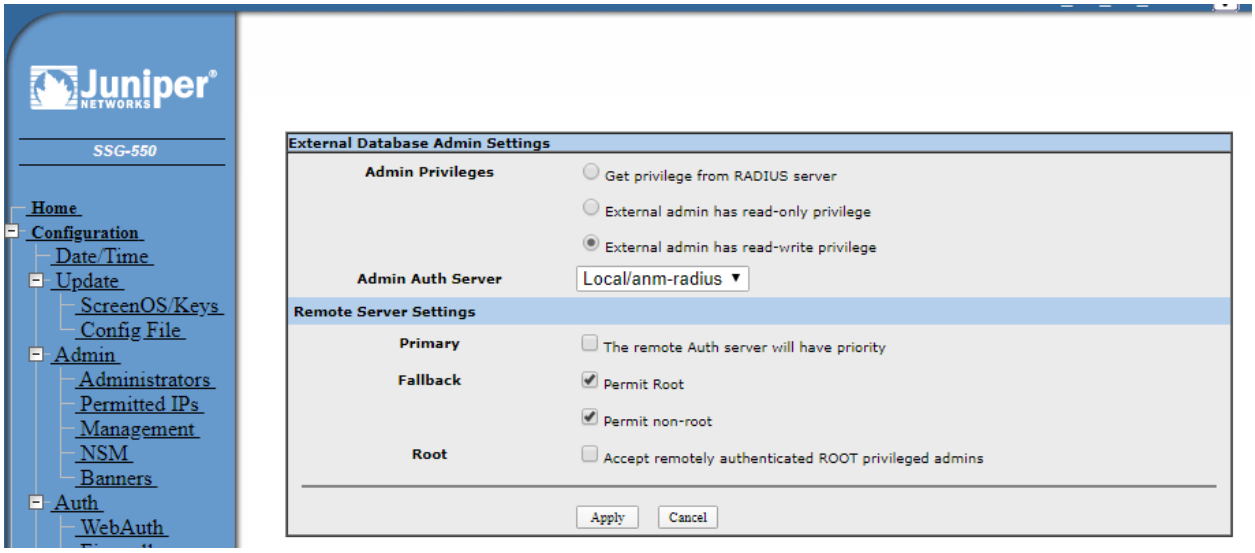
4.2. Yêu cầu về quản lý tài khoản

- Sử dụng hệ thống AAA để quản lý tài khoản người dùng tập trung (xác thực, phân quyền, ghi lịch sử tác động). Tối đa 02 tài khoản quản trị local dùng cho trường hợp khẩn cấp

- Trên GUI:
  - Cấu hình:
    - Chọn **Configuration > Auth > Auth Servers > Edit** > Click **New**
    - Nhập thông tin cho server: **Name, Type, Domain or IP address....> Save**



- Chọn **Configuration > Admin > Administrator.** Lựa chọn **Admin Auth Server** là server vừa khai báo > **Apply**



- Kiểm tra: Trong mục tương tự

- Quản trị viên phải sử dụng tài khoản được cấp riêng, phân quyền phù hợp trên local/AAA.

<u>Đối với tài khoản Local</u>

- Trên GUI:
  - Cấu hình:
    - Chọn **Configuration > Admin > Administrator >** Click **New**
    - Điền các thông tin về user và phân quyền phù hợp > Click **Apply**

      Privilege: Read-Only hoặc Read-Write

      Role:

      - Audit User: Có thể view cấu hình nhưng không thể sửa. Có thể view và clear Log.

      - Crypto user: Tương tự như Audit User nhưng không thể clear log. Có thể cấu hình certificates trên thiết bị.

      - Security user: Có thể chỉnh sửa toàn bộ các setting nhưng không thể clear log và cấu hình certificates
  - Trên CLI:

```
set admin user name_str password pswd_str [ privilege { read-write | read-only } ]
set admin user name_str role { audit | cryptographic | security }
```

  - Kiểm tra: Trong mục tương tự

<u>Đối với tài khoản AAA</u>

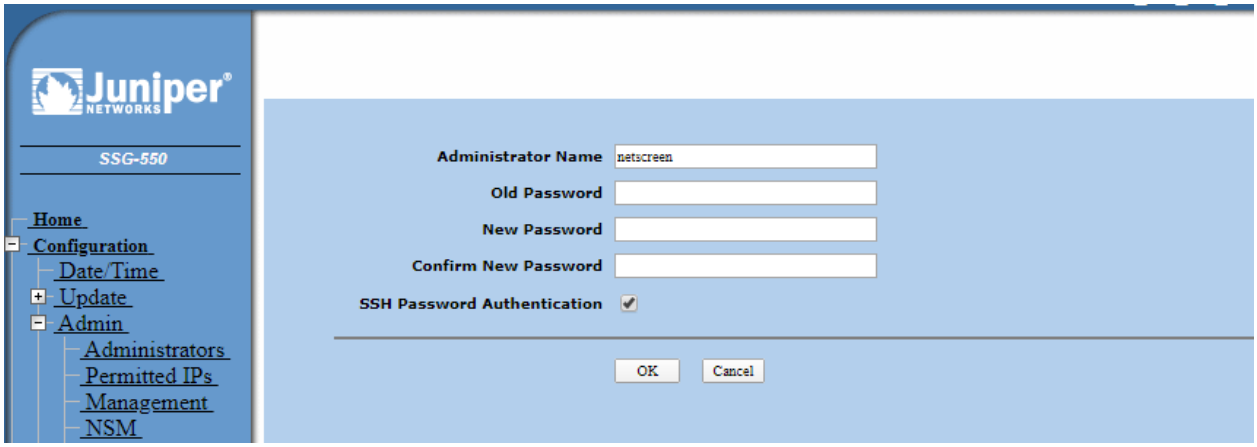
- Kiểm tra trực tiếp chính sách trên máy chủ AAA

- Đổi mật khẩu mặc định các tài khoản local của thiết bị

  - Trên GUI:

    - Cấu hình:

      - Chọn **Configuration > Admin > Administrator**
      - Trong hàng user **netscreen** click **Edit.** Điền đầy đủ thông tin và click **Apply**



    - Kiểm tra: Trong mục tương tự

- Thiết lập chính sách mật khẩu mạnh cho các tài khoản trên local/AAA.

Đối với account local

SSG550 không hỗ trợ thiết lập chính sách mật khẩu mạnh cho account local.

Đối với account AAA

  - Kiểm tra trực tiếp chính sách trên máy chủ AAA

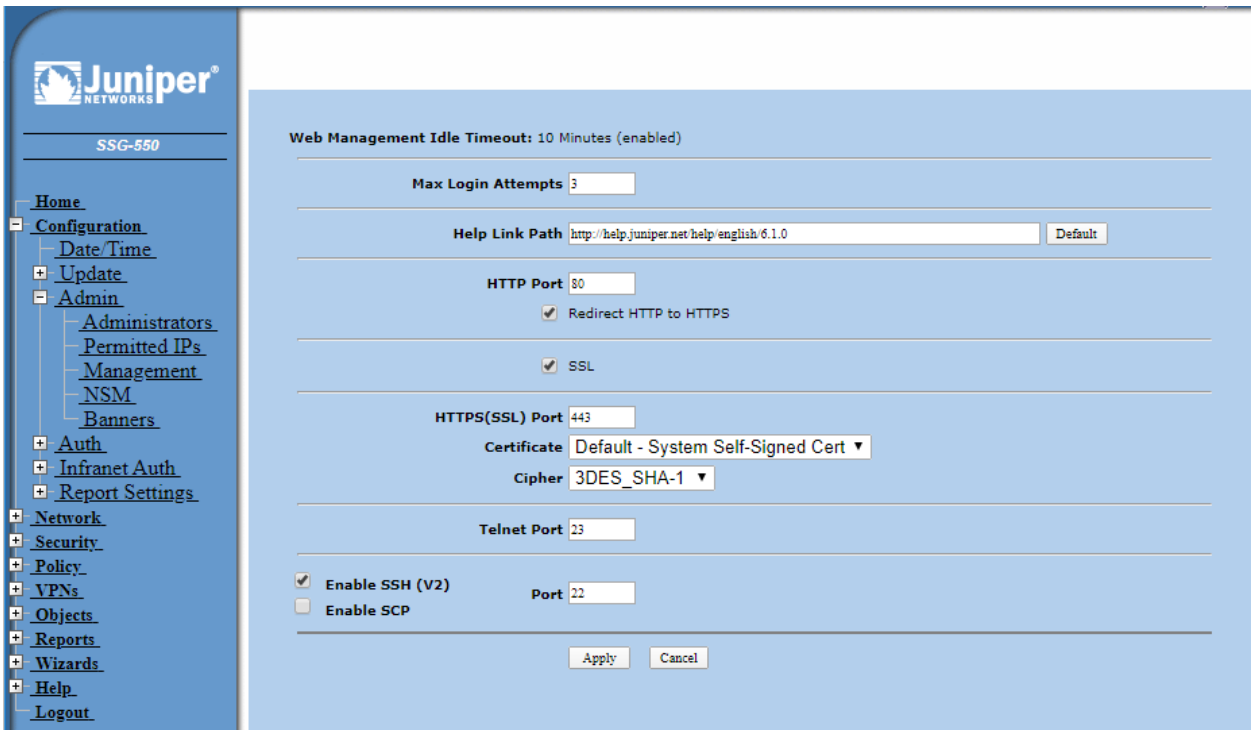
- Khóa sau 5 lần đăng nhập sai, thời gian khóa tài khoản do đăng nhập sai là 10 phút

Đối với account local

  - Trên GUI:

    - Cấu hình:

      - Chọn mục **Configuration > Admin > Management** > Nhập **Max login attempts: 5**



- Kiểm tra: Trong mục tương tự

Đối với account AAA

- Kiểm tra trực tiếp chính sách trên máy chủ AAA

4.3. Yêu cầu về kết nối quản trị

- Quản trị thiết bị qua VLAN quản trị dành riêng

- Kiểm tra trên cấu hình, đấu nối IP, quy hoạch VLAN quản trị

- Quản trị thiết bị qua kết nối trực tiếp Console hoặc kết nối từ xa an toàn, có mã hóa (SSHv2, HTTPS). Tắt các giao thức quản trị từ xa không an toàn (Telnet, HTTP)

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Configuration > Admin > Management**
    - Tick chọn **Redirect HTTP to HTTPS**
    - Tick chọn **enable SSH (v2)**
    - Xóa **Telnet port**
  - Kiểm tra: Trong mục tương tự

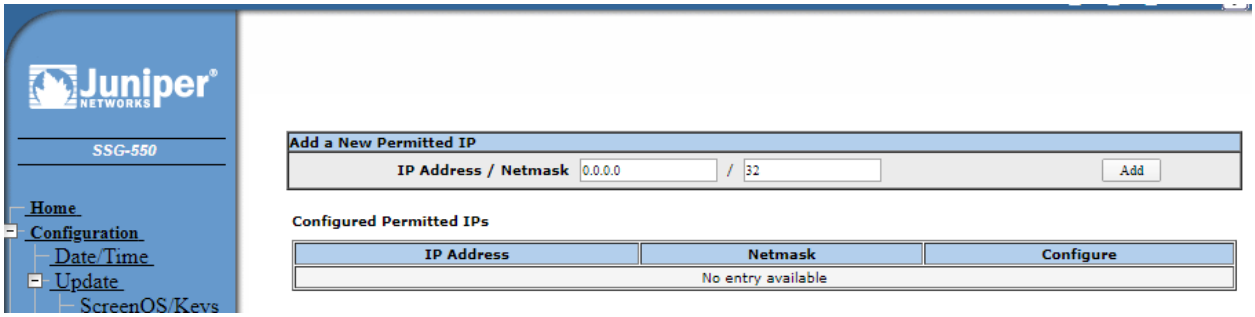
- Thời gian time-out của các phiên kết nối quản trị tối đa là 15 phút

- Trên CLI:

```
set admin auth web timeout 15
set console timeout 15
```

- Giới hạn chỉ cho phép quản trị từ các IP theo danh sách đăng kí

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Configuration > Admin > Permitted IPS/IDS >** Click **Add**
    - Điền thông tin IP/mask của máy quản trị và click **Apply**

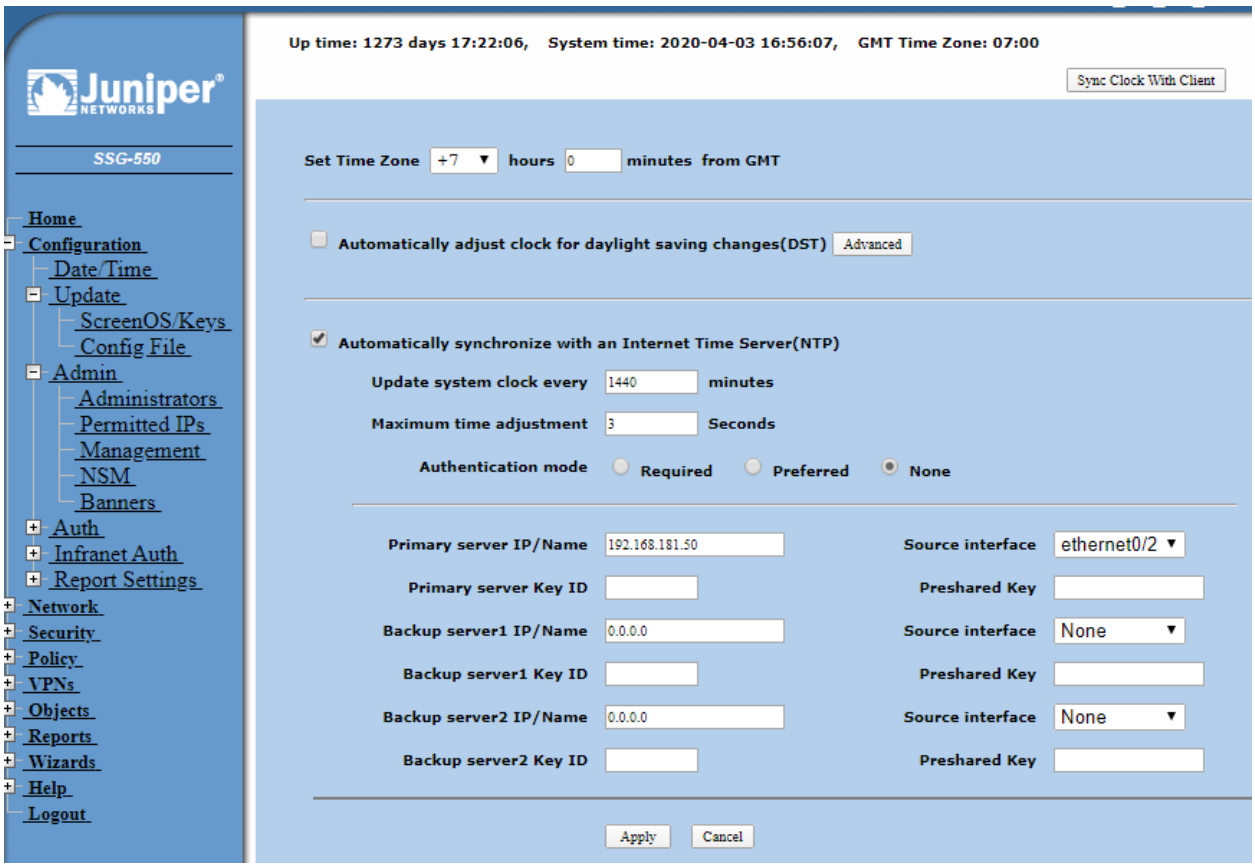


  - Kiểm tra: Trong mục tương tự

4.4. Yêu cầu cấu hình NTP

- Thiết bị phải được đồng bộ thời gian theo tối thiểu 01 máy chủ thời gian (NTP server)

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Configuration > Date/Time >** Nhập các thông số về NTP Server > **Click Apply**

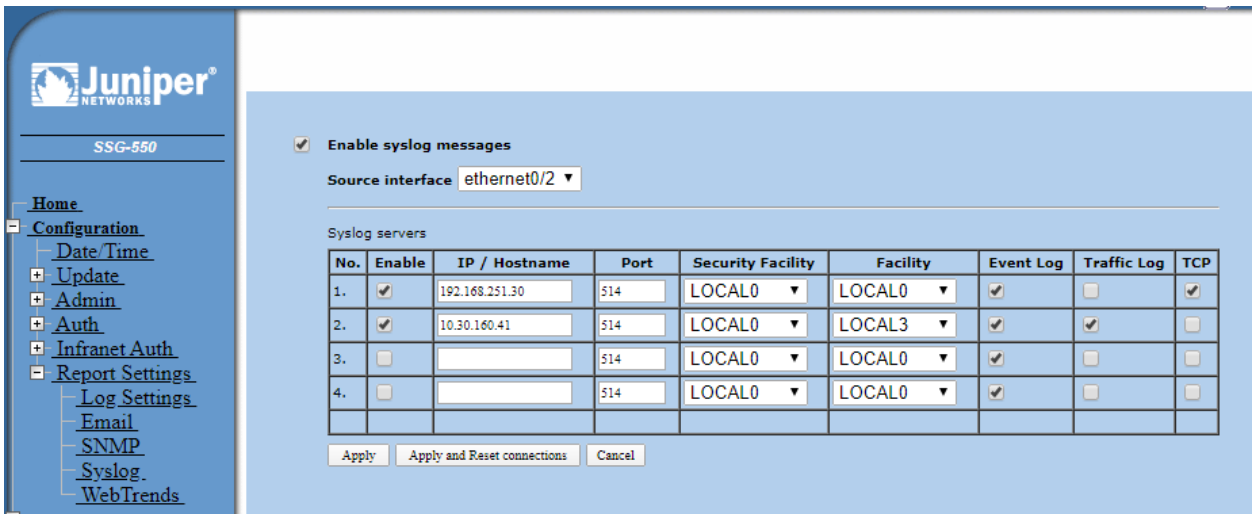


- Kiểm tra: Trong mục tương tự

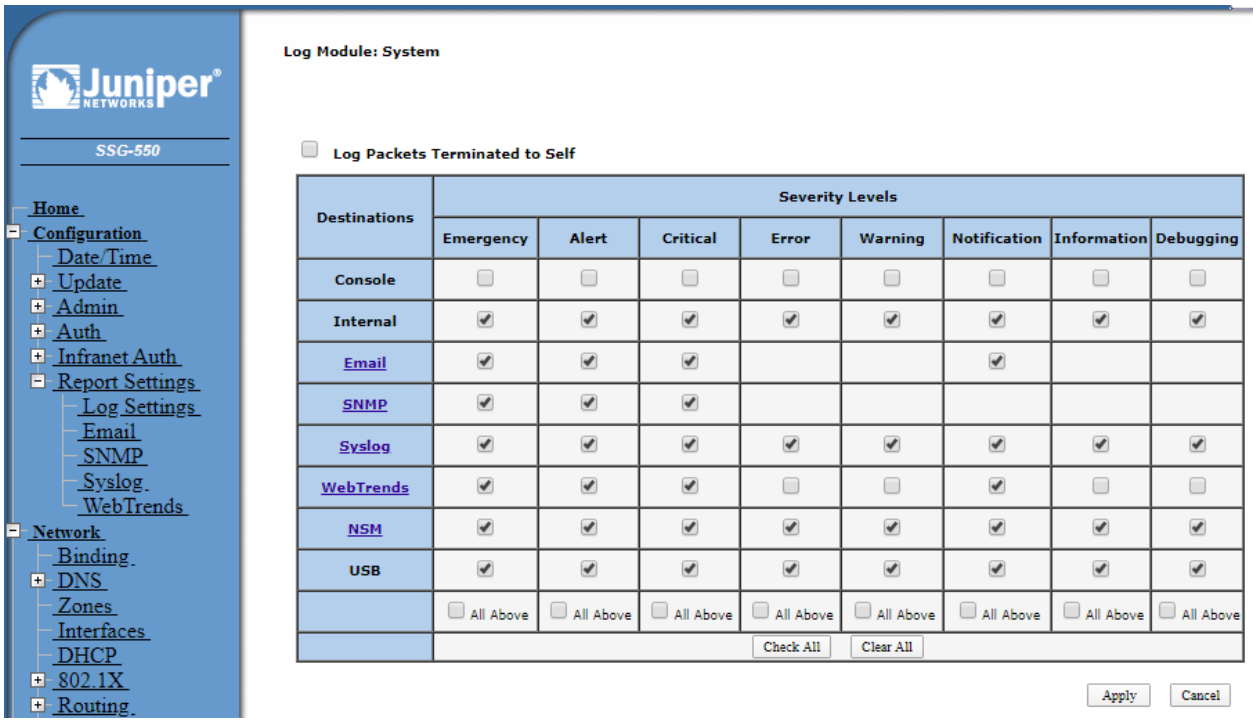
4.5. Yêu cầu cấu hình log

- Thiết bị phải được thiết lập bật chế độ ghi log và cấu hình lưu log tập trung tối thiểu 06 tháng. Trong trường hợp không có hệ thống lưu log tập trung thực hiện thiết lập lưu trên local

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Configuration > Report Settings > Syslog**
    - Tick chọn **Enable syslog message** và chọn **source interface** đẩy về svr lưu trữ
    - Nhập các thông tin về server syslog, loại log muốn đẩy về... > **Apply**



- Chọn mục **Configuration > Report Settings > Log Settings**
- Chọn các loại log cần lấy > **Apply**



- Kiểm tra: Trong mục tương tự

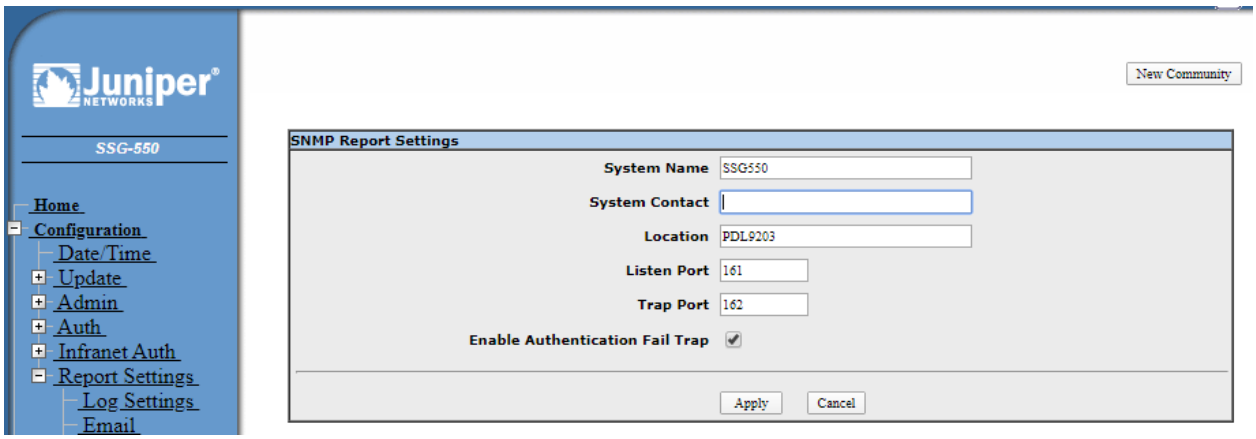
4.6. Yêu cầu cấu hình SNMP

- SNMP phiên bản v2c, v3. SNMP theo chế độ read-only. Community string SNMP riêng. Xóa bỏ community string mặc định. Chỉ cho phép truy cập SNMP từ máy chủ giám sát.

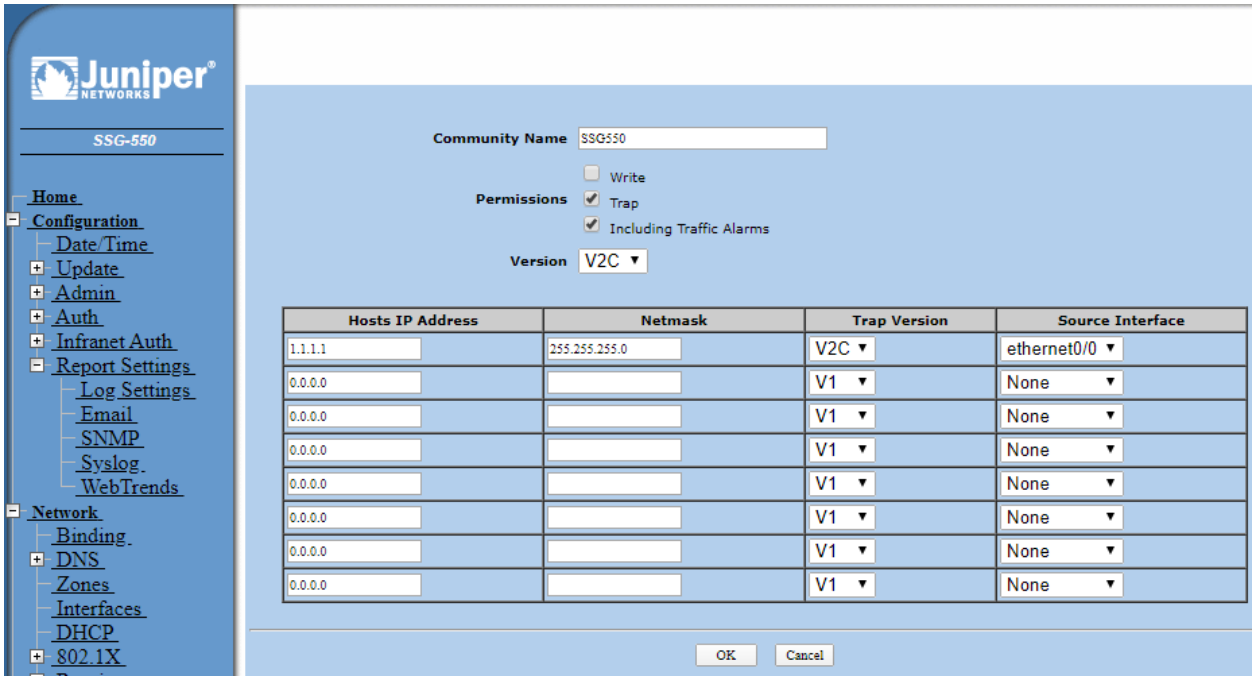
- Trên GUI:

- Cấu hình:

- Chọn **Configuration > Report Settings > SNMP>** Nhập các thông số của **SNMP**



- Chọn **Configuration > Report Settings > Click New Community**
- Chọn **Version V2C,** bỏ tick **Write,** Nhập thông tin về svr SNMP... > **OK**



- Kiểm tra: trong mục tương tự

5. Thiết lập các tính năng an ninh

5.1. Yêu cầu bật tính năng phòng chống tấn công mạng trên các Firewall

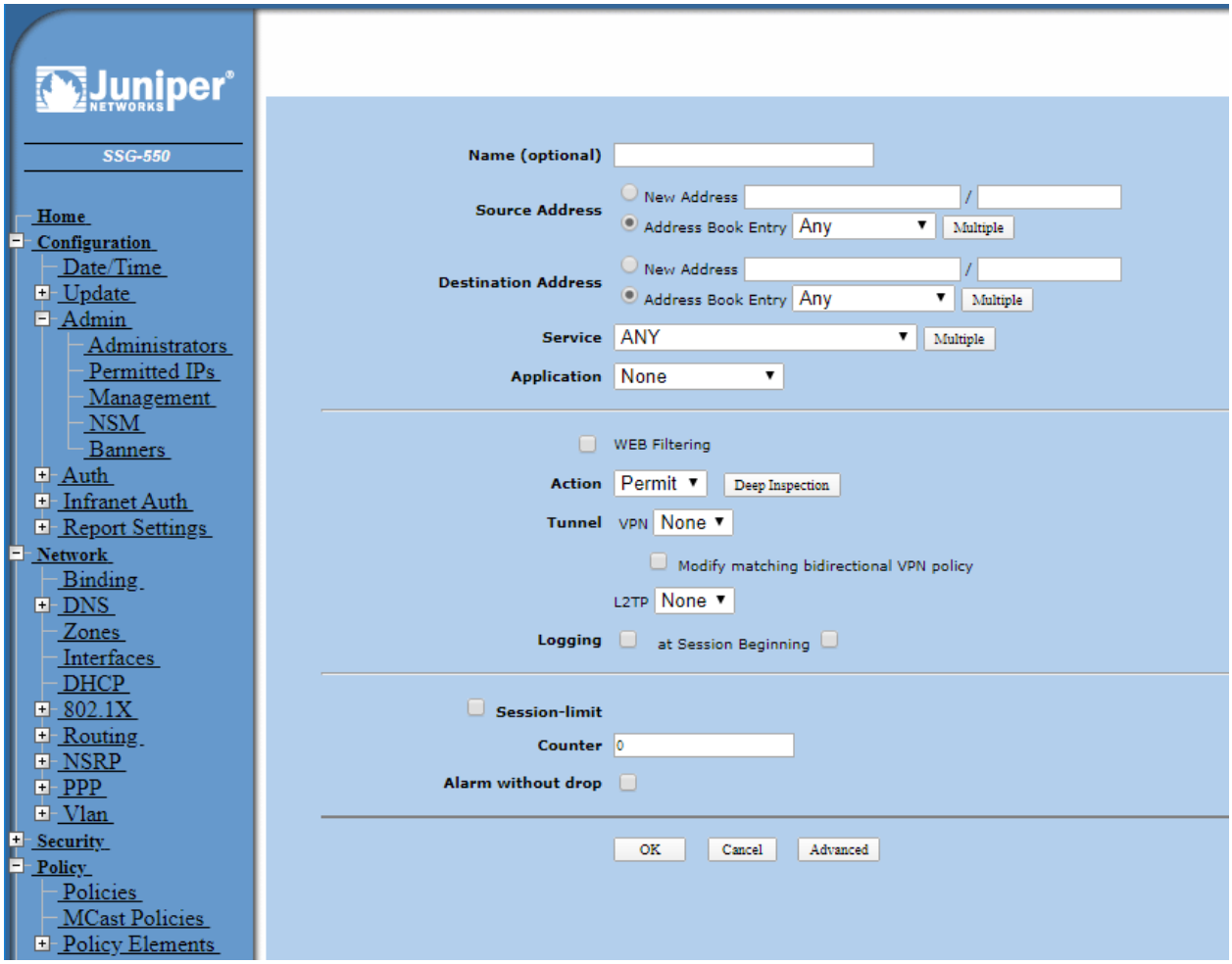
- Bật và cấu hình các tính năng phòng chống tấn công mạng phù hợp với hệ thống CNTT được Firewall bảo vệ (IPS/IDS, UTM, Screening)

Đối với IPS/IDS (Deep Inspection - DI):

- Yêu cầu phải có lisence để active feature và cập nhật Signature Pack của hãng để có list các Predefined-attack group hoặc có thể tự tạo các custom group attack theo ý muốn. Update manual có thể

tham khảo link sau:
https://services.netscreen.com/restricted/sigupdates

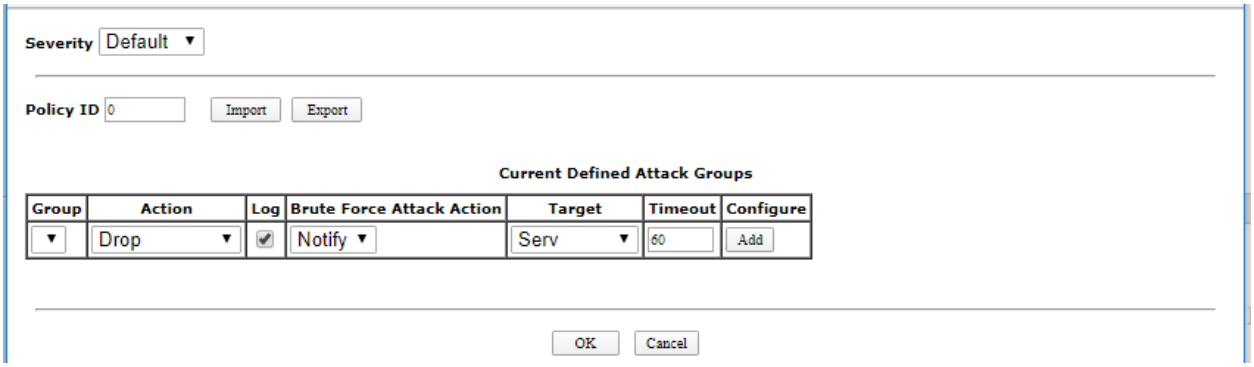
- Trên GUI:
  - Cấu hình:
    - Chọn **Policy** > **Policies** > Trong Policy cần thêm DI chọn **Edit** > **Deep Inspection**



- Chọn các thông số phù hợp > Click **OK**

  Group: Chọn các group attack phù hợp với policy. Ví dụ Chọn các group attack liên quan đến http cho policy mở truy cập đến các web svr...

  Action: Close (TCP-reset), Drop (packet), Ignore (tạo log và ngừng check), None.



- Kiểm tra: trong mục tương tự
- Trên CLI:

```
device-> set policy id 1
device(policy:1)-> set attack HIGH:HTTP:SIGS action close
device(policy:1)-> set attack MEDIUM:HTTP:ANOM action close
device(policy:1)-> exit
device-> save
```

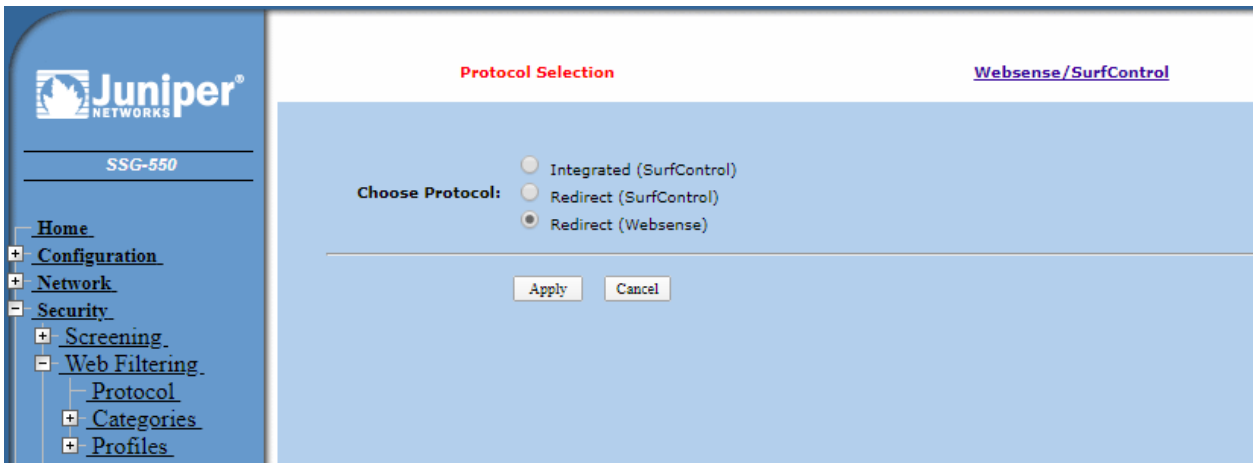
Đối với URL Filtering

- Yêu cầu phải có lisence để active full feature.
- ScreenOS cung cấp 2 Web-filtering solution:

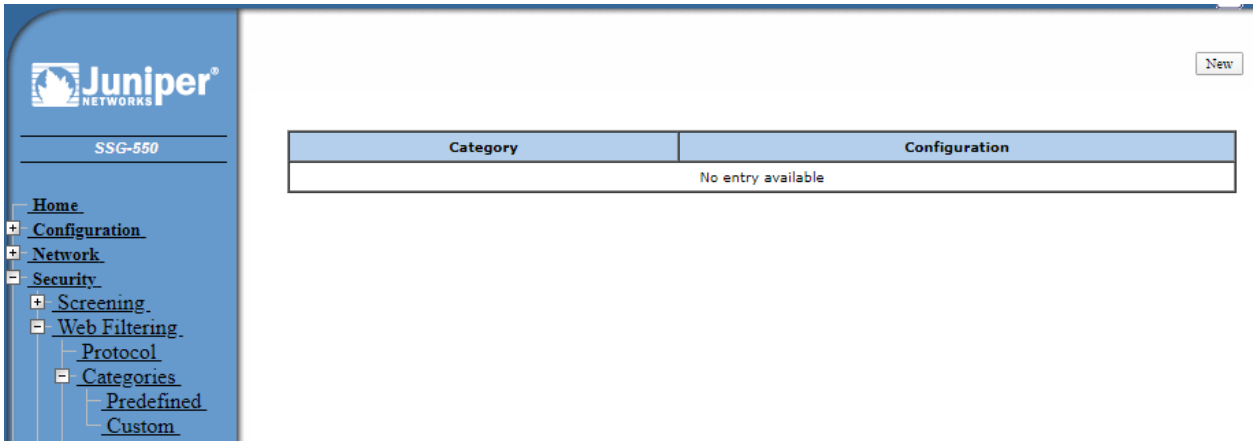
  Intergrated: Cho phép permit hoặc block truy cập bằng cách gán các Web-filtering profile (bao gồm danh sách các URL và action tương ứng) vào trong firewall policy.

  Redirect: Cho phép permit hoặc block truy cập bằng cách gửi các http request trong một phiên TCP với Websense svr hoặc Surf-Control svr. (Không hướng dẫn cấu hình trong tài liệu này)

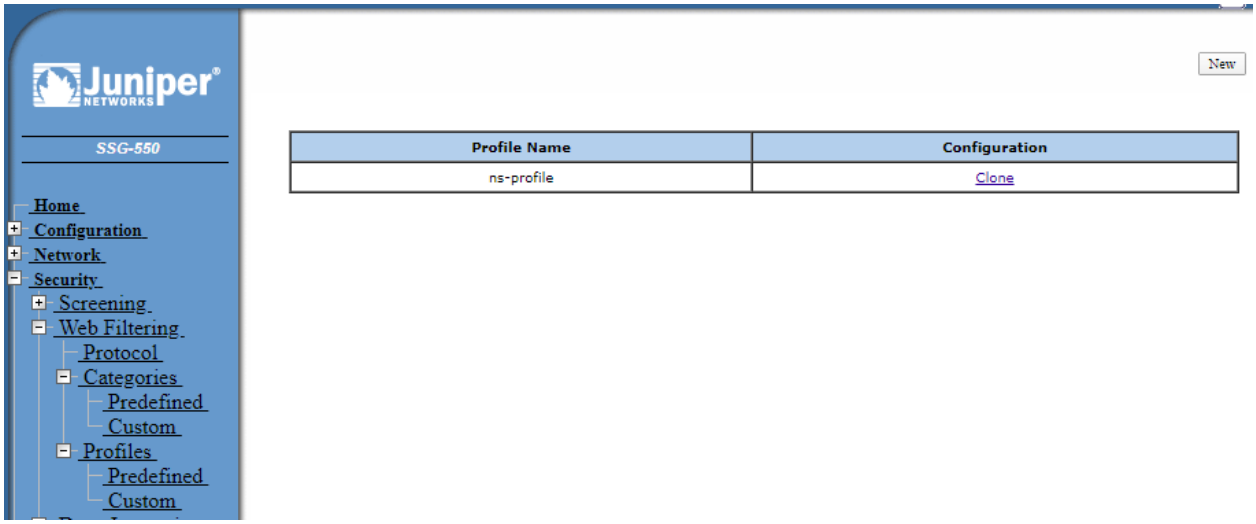
- Trên GUI:
  - Cấu hình:
    - Chọn **Security > Web Filtering > Protocol** > Tick chọn **Integrated (SurfControl)** > Click **Apply**
    - Tiếp tục tick chọn **Enable Web Filtering via CPA Server** > Click **Apply**



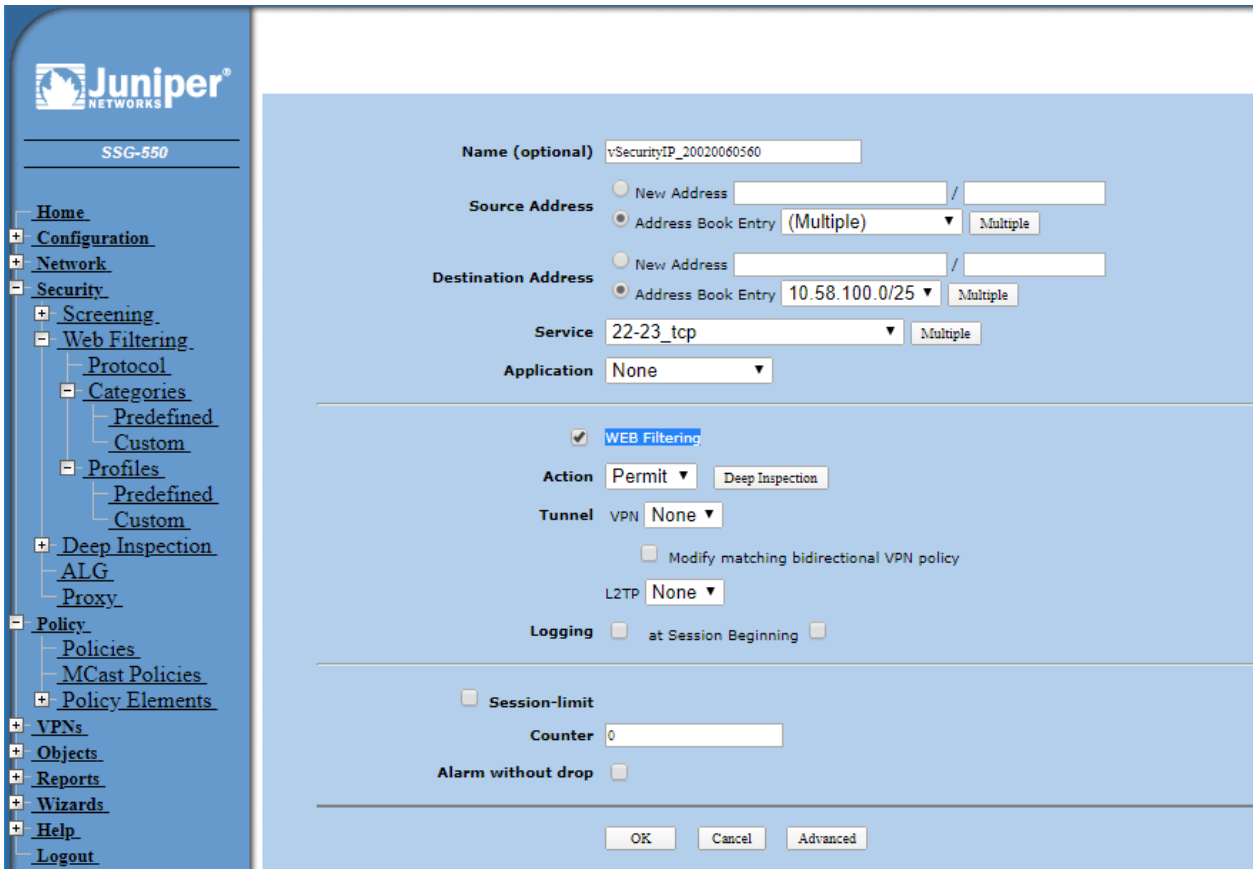
- Tạo URL categories: URL category là 1 danh sách các URL cùng 1 loại nội dung. Có thể sử dụng các URL categories đã được predefined của hãng hoặc có thể tạo mới bằng cách chọn **Security > Web Filtering > Categories > Custom > New** > Thêm các thông tin yêu cầu > **Apply**



- Tạo Profile: Bao gồm nhóm các URL categories được gán với 1 hoặc nhiều action**.** Có thể sử dụng Profile mặc định của hãng (ns-profile) hoặc có thể tạo mới bằng cách chọn **Security > Web Filtering > Profiles > Custom > New** > Thêm các thông tin yêu cầu (URL, action…) > **Apply**



- Gán Profile vào Policy: Chọn **Policy** > **Policies** > Trong Policy cần thêm Web-filtering tick chọn **WEB Filtering** > **chọn** Profile tương ứng > **Click OK**



- Kiểm tra: trong mục tương tự
- Trên CLI:

1. Web Filtering

get url

device->set url protocol sc-cpa

device(url:sc-cpa)-> set enable

device(url:sc-cpa)-> set group-based-filtering

device(url:sc-cpa)-> get user-group group_name | all

2. URL Category

device(url:sc-cpa)-> set category competitors url www.comp1.com

device(url:sc-cpa)-> set category competitors url www.comp2.com

3. Web-Filtering Profile

device(url:sc-cpa)-> set profile my-profile other permit

device(url:sc-cpa)-> set profile my-profile competitors block

device(url:sc-cpa)-> exit

4. Firewall Policy

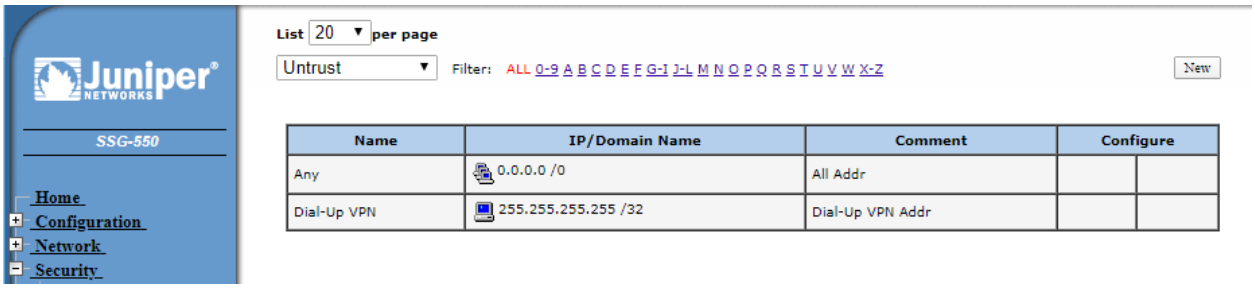
device-> set policy id 23 from trust to untrust any any http permit url-filter

```
device-> set policy id 23
device(policy:23)-> set url protocol sc-cpa profile my-profile
device(policy:23)-> exit
device-> save
```

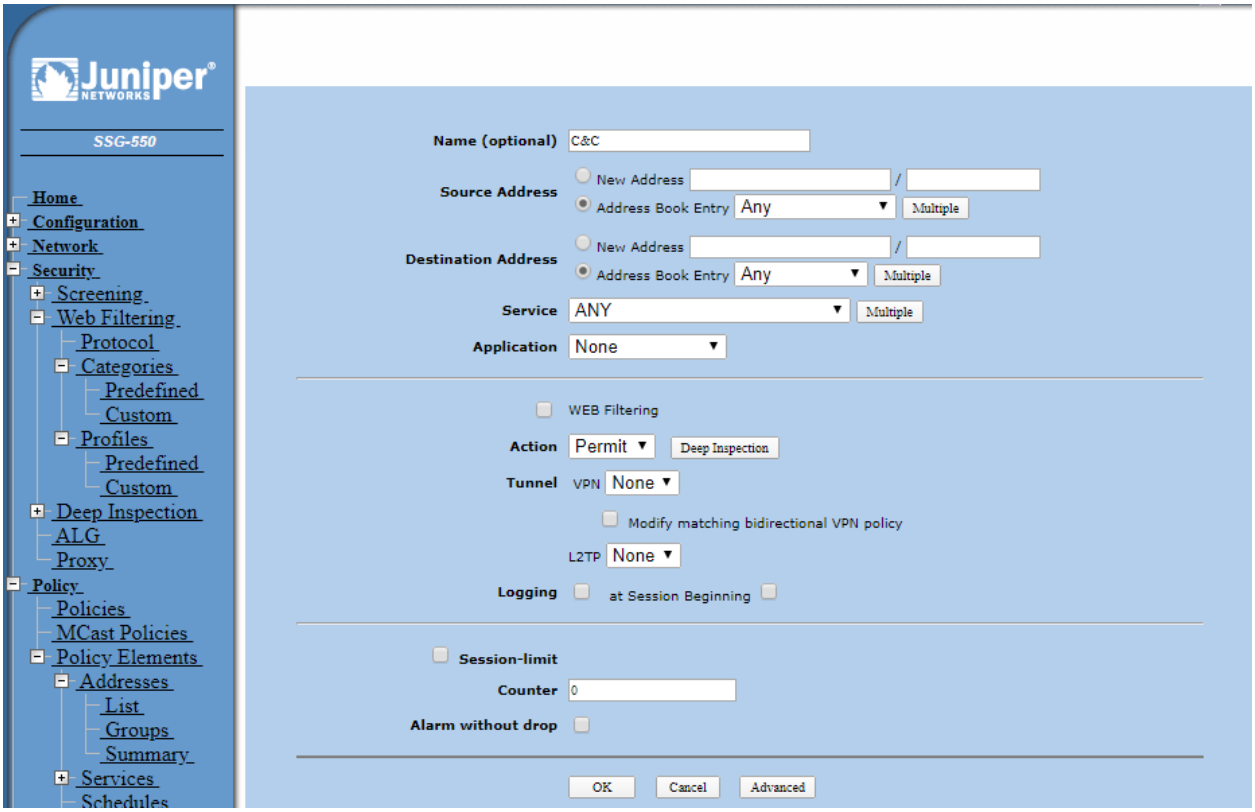
5.2. Yêu cầu rule phát hiện và ngăn chặn các kết nối C&C

- Khai báo phát hiện và ngăn chặn các kết nối C&C, các domain độc hại. Khai báo rule ở vị trí có hiệu lực đầu tiên

- Cấu hình:
  - Chọn mục **Policy** > **Addresses** > **List** > Click **New**



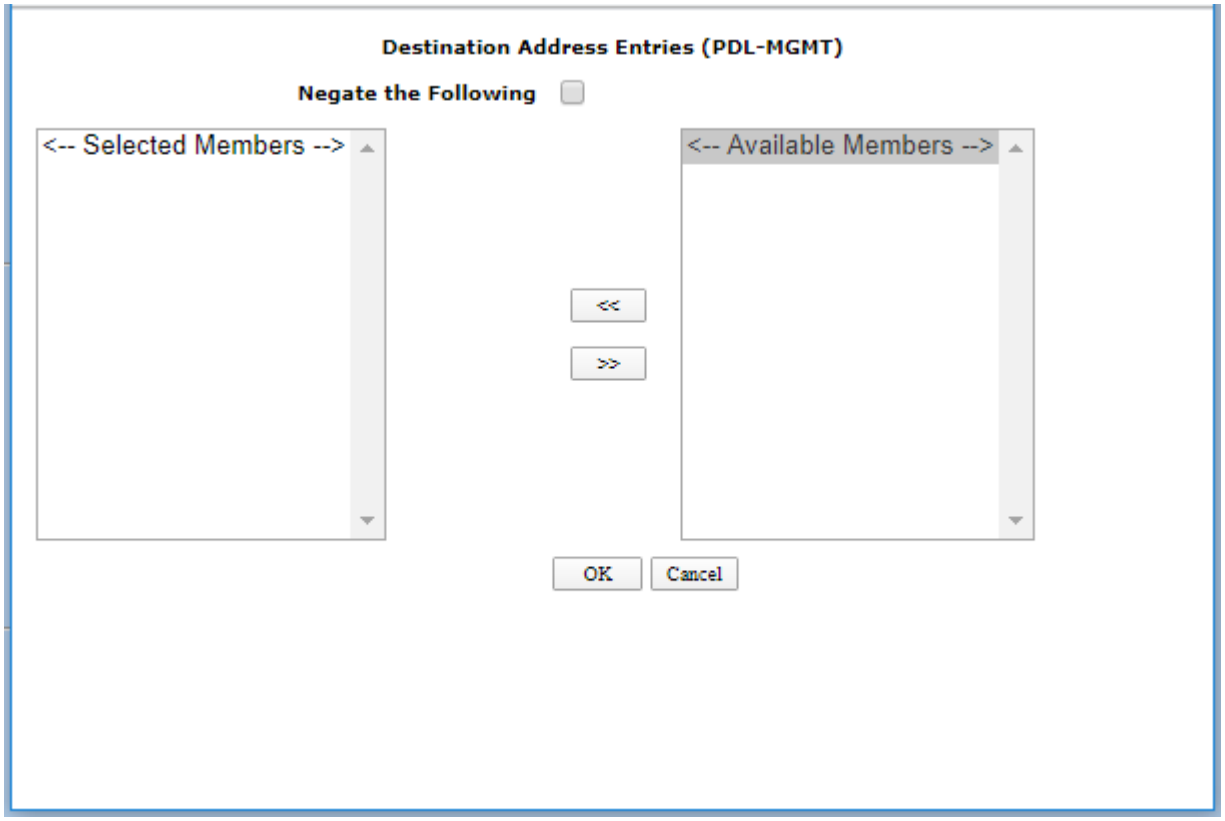
  - Nhập các tham số để tạo danh sách địa chỉ IP C&C > Click **OK**
  - Tạo Rule trong kết nối từ zone Trust đến Untrust: Chọn mục **Policy** > **Policies** > Click **New**



  - Điền các tham số:

    Source Address: Any

Destination Address: Chọn **Multiple** > Thêm các IP C&C đã tạo vào > Click **OK**



Service: Any

Action: Deny

Tick chọn **Logging** > Click **OK**

- Kiểm tra: trong mục tương tự

5.3. Yêu cầu rule phát hiện và chặn người dùng quản trị ra Internet

- Khai báo rule phát hiện và chặn người dùng quản trị ra Internet trực tiếp và qua Proxy, chỉ mở cho người dùng quản trị đến các hệ thống theo các port quản trị TCP-22 (SSH), (TCP-23 (Telnet), TCP-3389 (RDP),1433 (MS-SQL), TCP-1521->1527 (Oracle), TCP-3306 (Mysql), TCP-5432 (postgresql), TCP/UDP-161/162 (SMTP)

- Cấu hình:
  - Tương tự như mục trên: Các tham số cần điền:

    Source Address: dải IP của người dùng quản trị

    Destination Address: Any

    Service: Any

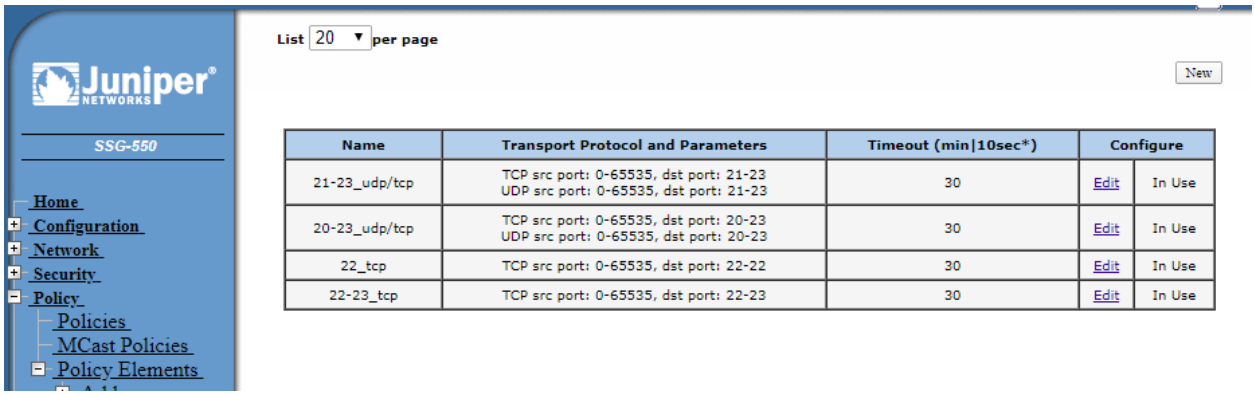
    Action: Deny

    Tick chọn **Logging** > Click **OK**
- Kiểm tra: trong mục tương tự

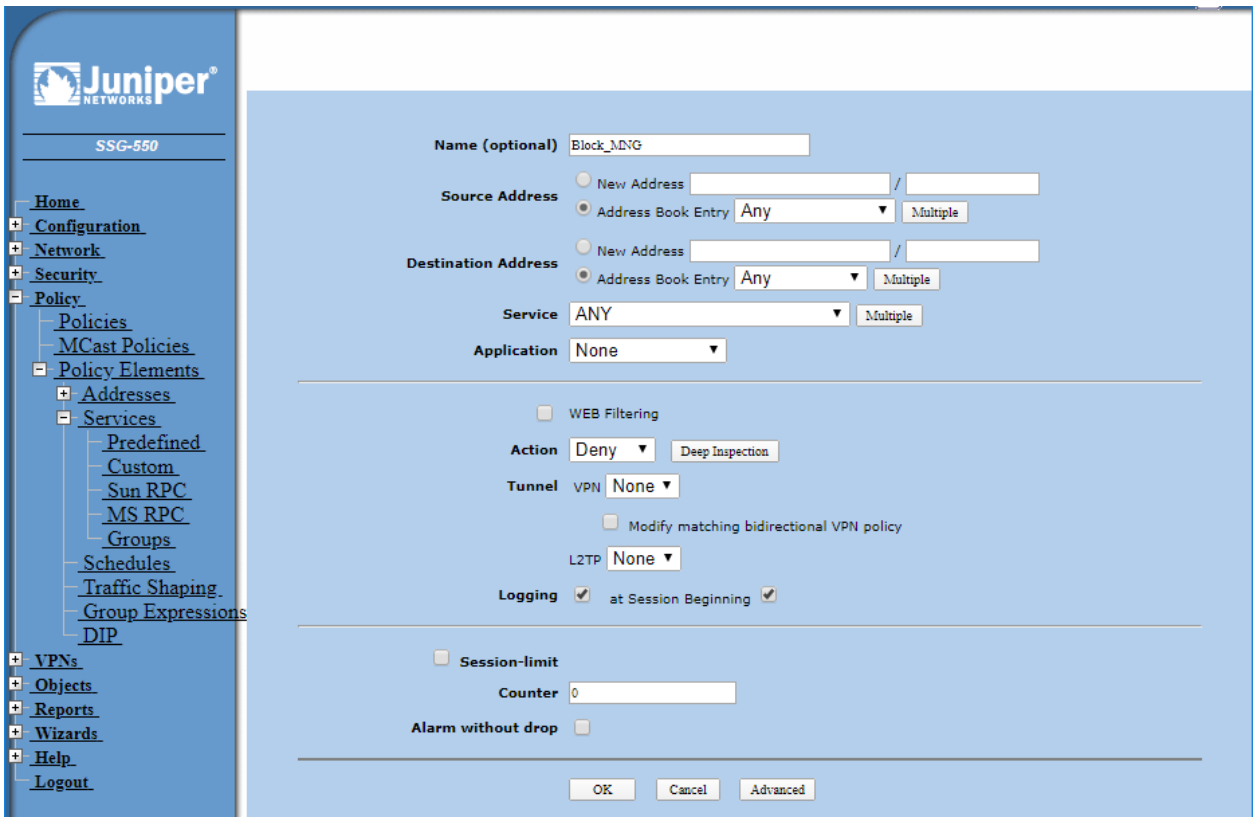
5.4. Yêu cầu rule phát hiện và chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao

- Khai báo rule phát hiện và chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao:

  - Internet: Level 1
  - Wan: Level 2
  - Office: Level 3
  - DMZ: Level 4
  - Server Farm: Level 5
  - Cấu hình:
    - Khai báo danh sách các port quản trị: Chọn mục **Policy** > **Services** > **Policy Elements** > **Custom** > **New** > Tạo danh sách các port quản trị > **Apply**



  - Tạo Rule trong kết nối từ zone security level thấp đến cao: Chọn mục **Policy** > **Policies** > Click **New**



- Các tham số cần điền:

  Source Address: Any

  Destination Address: Any

  Service: Chọn group service vừa tạo

  Action: Deny

  Tick chọn **Logging** > Click **OK**

- Kiểm tra: trong mục tương tự

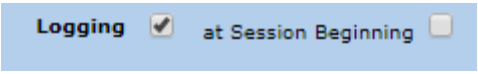
5.5. Yêu cầu rule khai báo Policy vừa đủ các địa chỉ nguồn, địa chỉ đích và port dịch vụ

- Với port quản trị:
  - Mở chi tiết và cụ thể theo ip người dùng và hệ thống được cấp phép trên Firewall Office, Firewall WAN
  - Mở theo dải không qua subnet 24 trên Firewall Server Farm, Firewall DMZ
- Với các port khác:
  - Mở không quá subnet 16
  - Mở không quá range 2000 port
- Với kết nối internet:
  - Được phép mở bất kỳ đích đến với kết nối đi internet

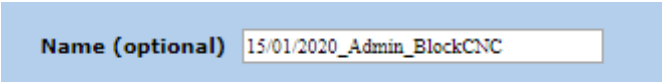
5.6. Yêu cầu rule khai báo phải chứa các thông tin phục vụ kiểm tra và rà soát ATTT

- Khi mở rule cần chú ý mở đúng theo: Title, zone, tags,...

- Các rule quan trọng phải bật lưu logs hoặc bật lưu logs trên tất cả các rule đối với thiết bị nào đang đẩy về hệ thống phân tích logs tập trung



- Các rule cần phải có comment rõ ràng: ngày/tháng/năm mở rule - tên quản trị - rule mở cho mục đích gì - rule mở tạm thời thì cần có thời hạn cụ thể.



- Kiểm tra: trong mục tương tự

5.7. Yêu cầu IPS/IDS phải update bộ rule mới nhất và đầy đủ

- IPS/IDS phải update bộ rule mới nhất và đầy đủ được ban hành trên website và hệ thống cập nhật của hãng

- Cấu hình:
  - Chọn **Configuration > Update > Attack Signature >** Điền các thông tin **> click OK**

    Signature Pack: Chọn gói pack muốn sử dụng **(Default: Base))**

    Update Mode: Chọn **Automatic Update**

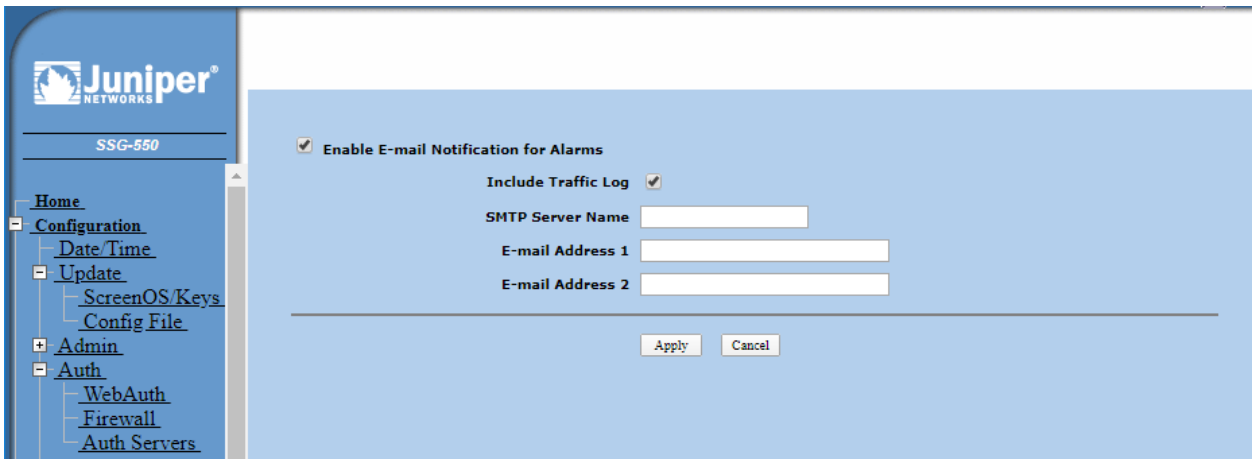
    Schedule: Chọn ngày định kỳ update

    Time (hh:mm): Chọn thời điểm định kỳ để update
- Kiểm tra: trong mục tương tự

5.8. Yêu cầu thiết lập gửi mail cảnh báo

- Thiết lập gửi mail cảnh báo về người quản trị khi có hành động phát hiện và chặn xâm nhập

- Cấu hình:
  - Chọn mục **Configuration > Report Settings > Email**
  - Thiết lập các tham số cấu hình Email cảnh báo > **Save**



- Kiểm tra: trong mục tương tự.

III. Hướng dẫn cho firewall SOPHOS XG

1. Yêu cầu chung

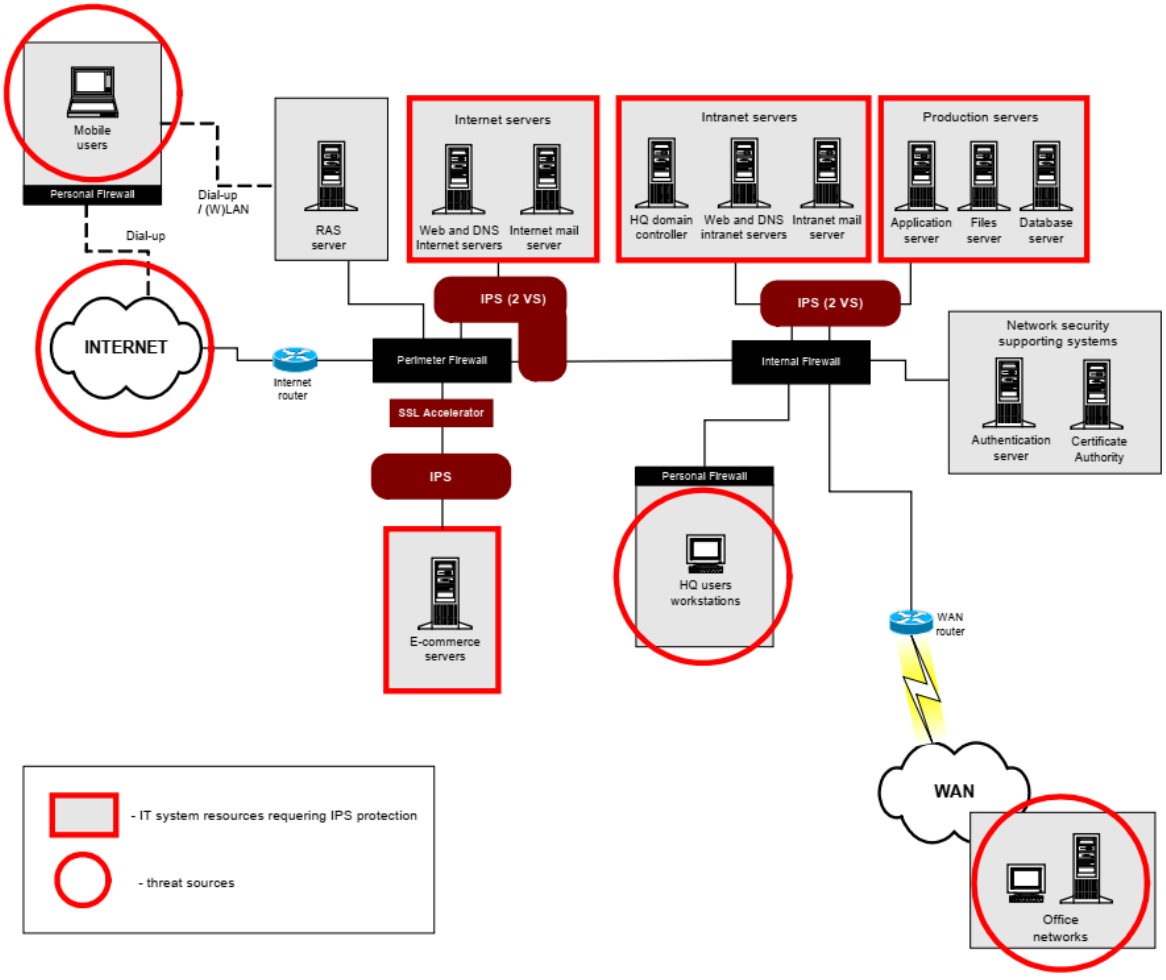
1.1. Yêu cầu phát hiện và chống tấn công từ internet

- Phải đặt IPS/IDS tại các vùng mạng mà monitor được tất cả các traffic in/out internet

  - Đặt tại vùng DMZ kết nối internet
  - Đặt tại vùng người dùng truy cập Internet.

- Phải đặt Firewall giữa kết nối từ Internet vào mạng nội bộ, đảm bảo toàn bộ traffic in/out internet phải đi qua Firewall

  - Đặt tại vùng DMZ kết nối internet
  - Đặt tại vùng người dùng truy cập Internet.



1.2. Yêu cầu phát hiện và chống tấn công từ nội bộ

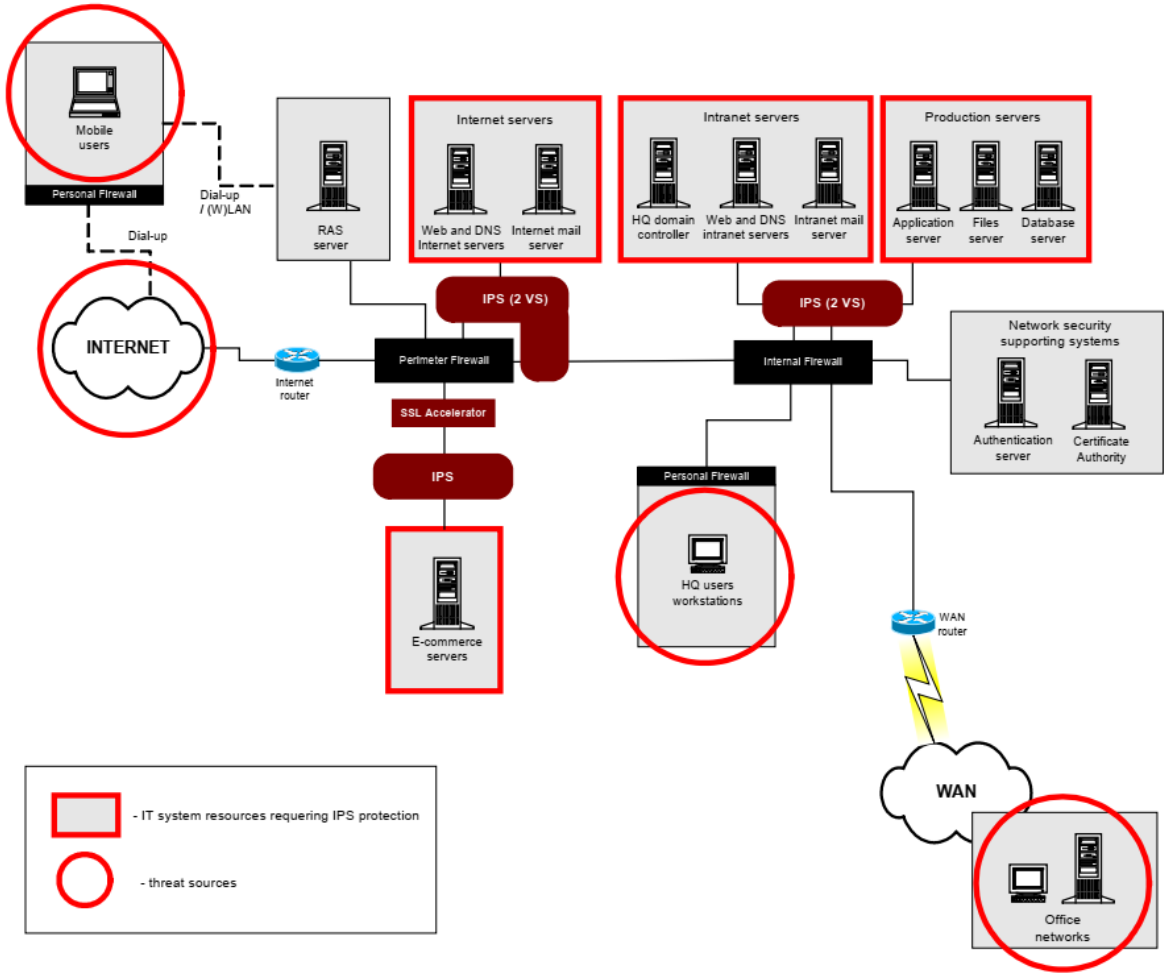
- Phải đặt IPS/IDS tại các vùng mạng mà monitor được tất cả traffic in/out các hệ thống cần bảo vệ

  - Đặt tại vùng Office kết nối vào mạng nội bộ.
  - Đặt tại vùng WAN kết nối vào mạng nội bộ.

- Đặt tại vùng Server Farm kết nối vào mạng nội bộ.
- Đặt tại vùng Partner kết nối vào mạng nội bộ.

- Phải đặt Firewall giữa kết nối từ các hệ thống khác tới hệ thống cần bảo vệ, đảm bảo toàn bộ traffic in/out của vùng mạng cần bảo vệ đi qua Firewall

- Đặt tại vùng Office kết nối vào mạng nội bộ.
- Đặt tại vùng WAN kết nối vào mạng nội bộ.
- Đặt tại vùng Server Farm kết nối vào mạng nội bộ.
- Đặt tại vùng Partner kết nối vào mạng nội bộ.



2. Cấu hình an ninh lớp 1

2.1. Yêu cầu shutdown port không sử dụng

- Shutdown tất cả các port không sử dụng trên thiết bị, chỉ bật lên khi có yêu cầu sử dụng

- Dòng Sophos XG firewall không hỗ trợ disable interface vật lý. (Hỗ trợ trên dòng Sophos UTM)

2.2. Yêu cầu mô tả kết nối rõ ràng

- Cổng đang bật phải có mô tả kết nối rõ ràng xác định được thông tin đấu nối của thiết bị đầu xa

    - Dòng Sophos XG firewall không hỗ trợ mô tả cho interface vật lý. (Chỉ có thể thêm mô tả với interface bridge)

3. Cấu hình an ninh lớp 3

3.1. Xác thực cho các giao thức lớp 3

- VRRP, HSRP, GLBP, NSRP phải cấu hình xác thực cho giao thức giữa các thiết bị. Sophos XG Firewall hiện tại chưa hỗ trợ các tính năng như VRRP.

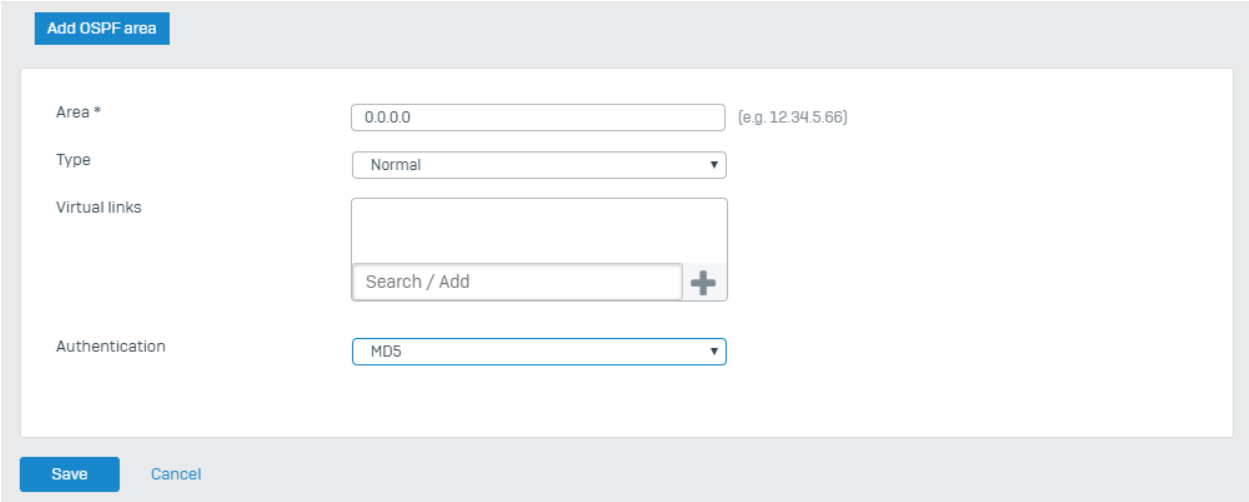
- OSPF phải thiết lập chuỗi xác thực có mã hóa giữa 2 thiết bị.

    - Trên GUI:

        - Cấu hình:

            - Chọn mục Chọn mục **Configure > Routing > tab OSPF**

            - Trong phần **Area >** click vào biểu tượng tại Area cần cấu hình

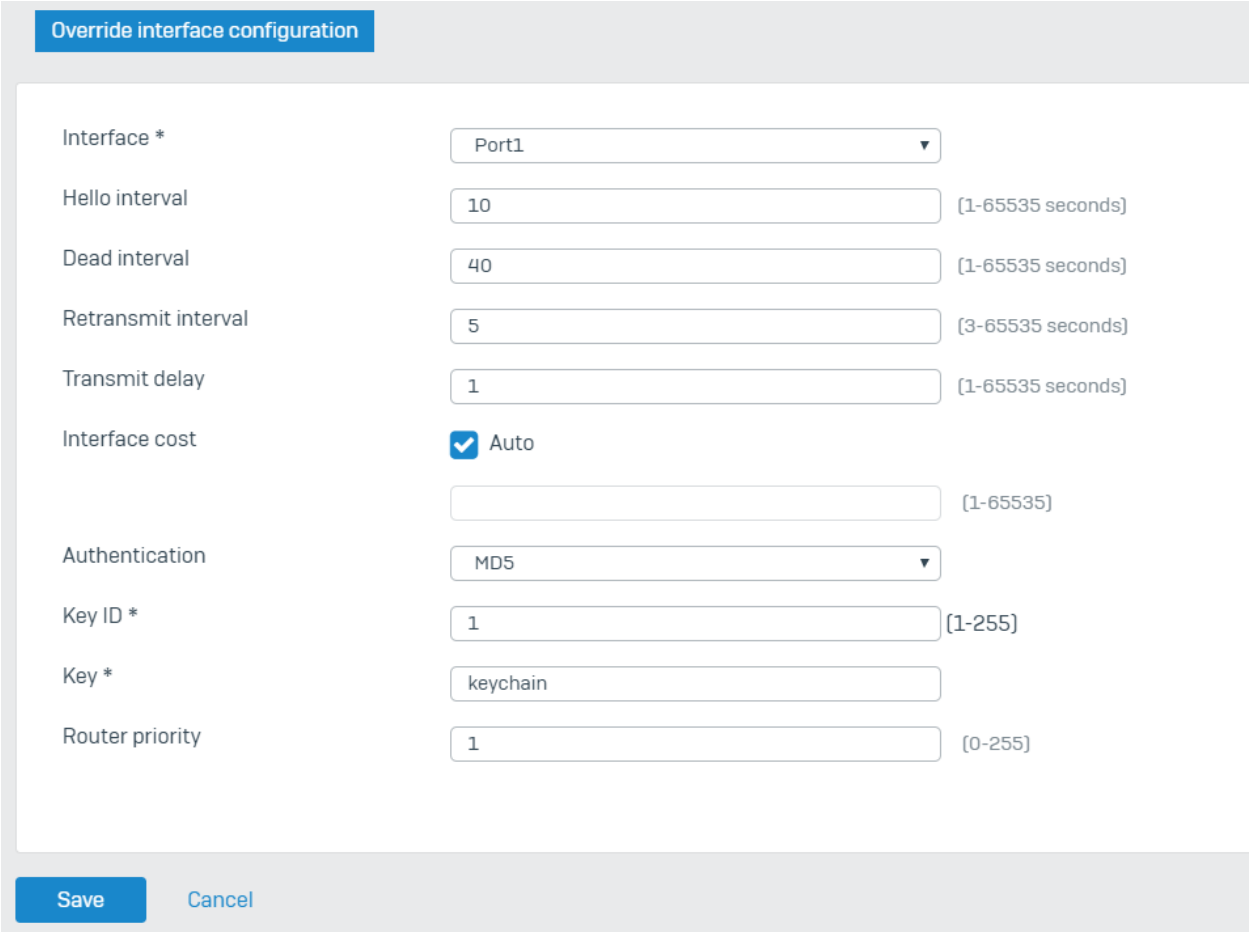


            - **Authentication:** Chọn **MD5** > **Save**

            - **Trong phần Interface >** click vào biểu tượng tại Interface cần cấu hình

            - **Authentication:** Chọn **MD5**

            - Điền ID và MD5-key > Click **Save**



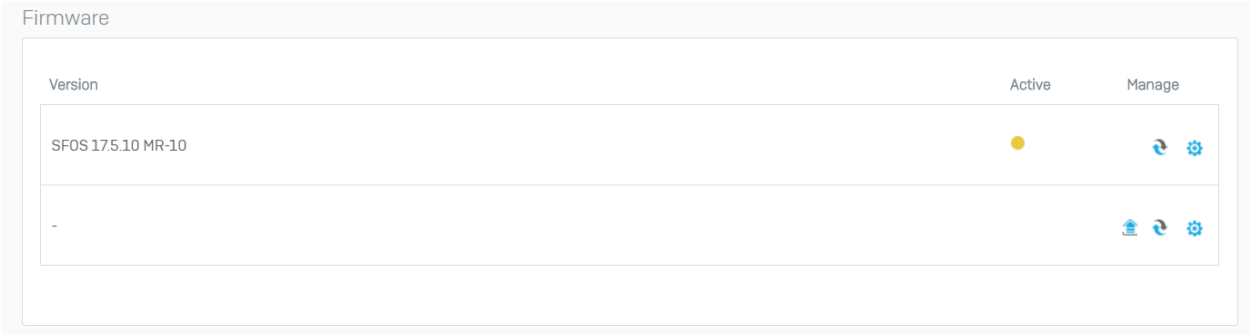
- Kiểm tra: Trong mục tương tự

- Chuỗi xác thực:
  - Có độ phức tạp bao gồm chữ in thường, in hoa, ký tự
  - Chuỗi dài hơn 10 ký tự
  - Không đặt các mật khẩu dễ đoán
- BGP phải thiết lập chuỗi xác thực có mã hóa giữa 2 thiết bị.
  - Sophos XG Firewall không hỗ trợ xác thực BGP.

4. Cấu hình quản trị

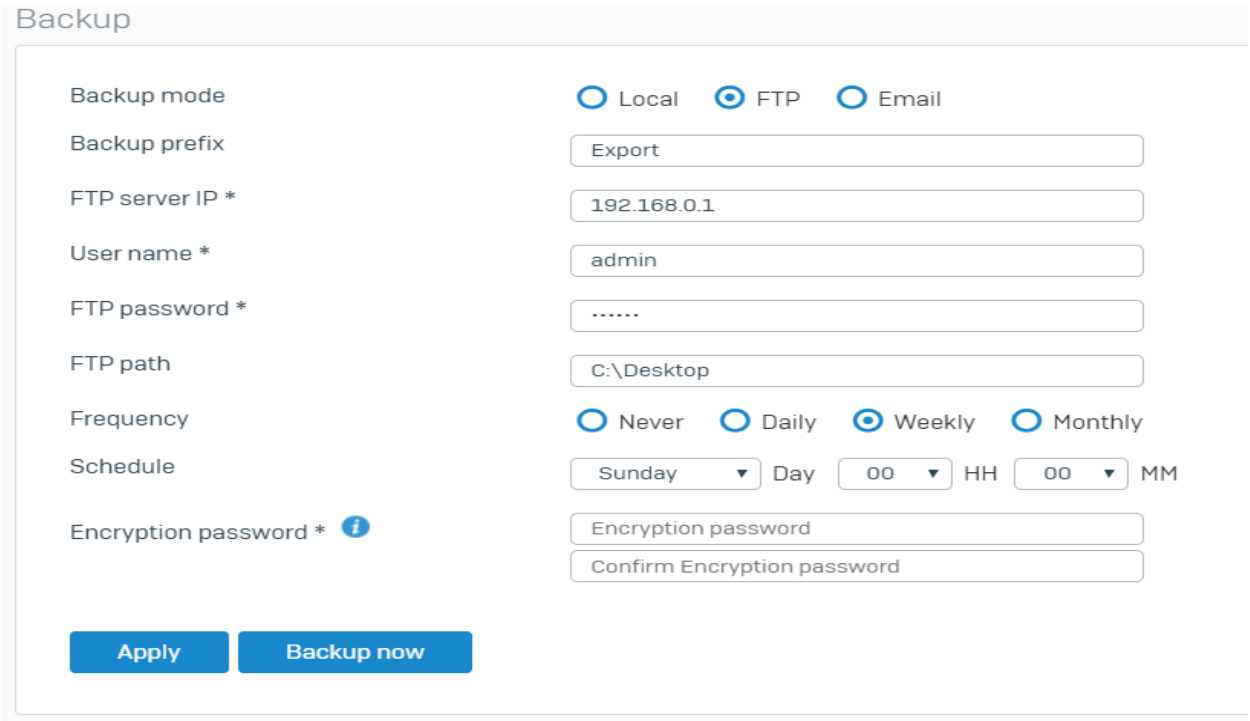
4.1. Yêu cầu về sao lưu cấu hình

- Thiết bị phải được sử dụng phiên bản hệ điều hành và cập nhật các bản vá đảm bảo an toàn theo yêu cầu của bộ phận ATTT.
  - Trên GUI:
    - Chọn mục **System > Backup & Firmware**

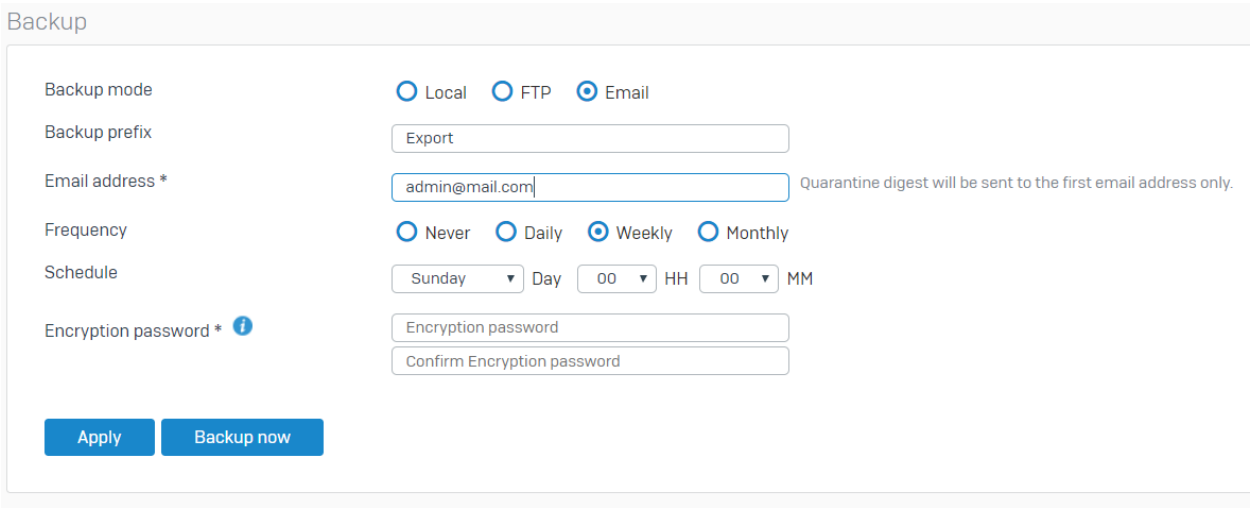


- Lưu cấu hình trước khi tác động và định kì tối thiểu 01 lần/tuần. Lưu tối thiểu 02 bản gần nhất. Không lưu bản sao lưu trên máy tính cá nhân của quản trị viên.

- Trên GUI:
  - Chọn mục **System > Backup & Firmware > tab Backup & Restore**
  - Đối với backup qua FTP: Tick chọn **FTP**



  - Điền các thông tin về SVR FTP
  - **Frequency** chọn **weekly** > **Apply**
  - Tương tự đối với backup qua email



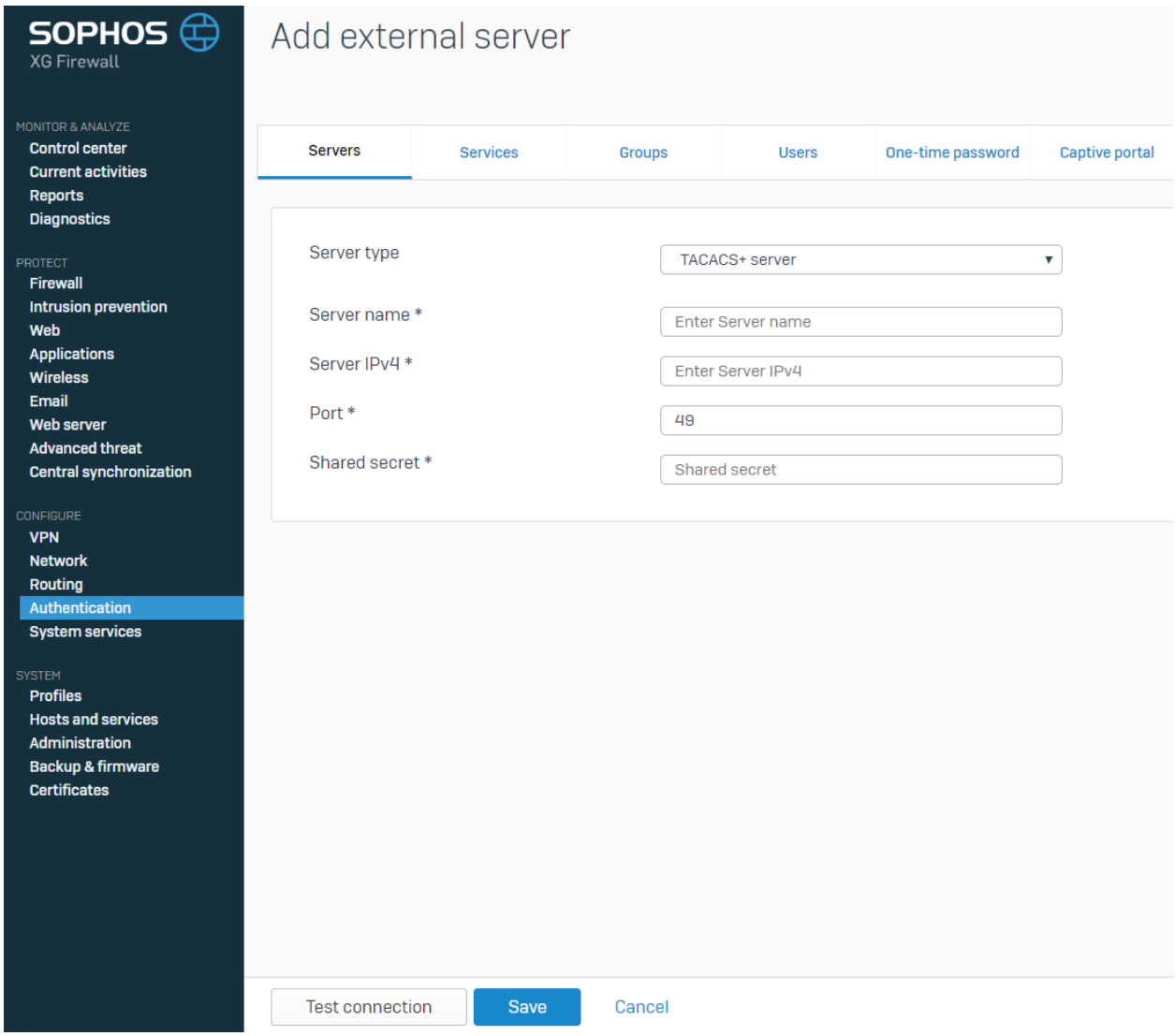
- Kiểm tra: Kiểm tra file cấu hình được lưu trên máy tính đích hoặc email.

4.2. Yêu cầu về quản lý tài khoản

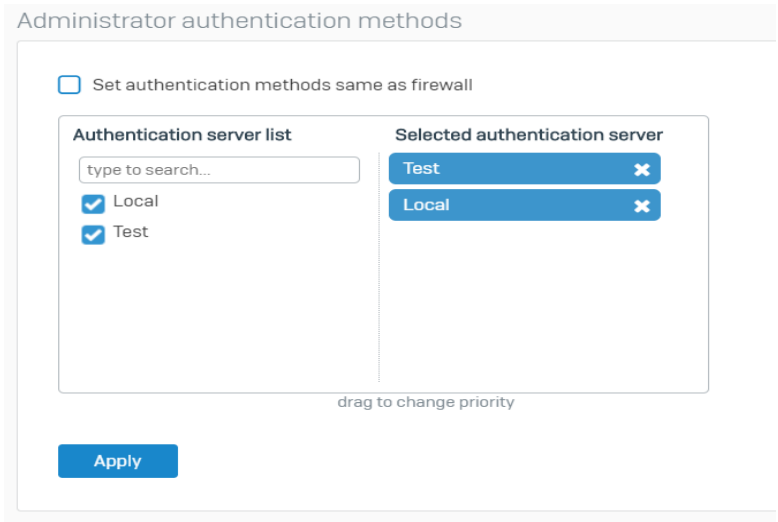
- Sử dụng hệ thống AAA để quản lý tài khoản người dùng tập trung (xác thực, phân quyền, ghi lịch sử tác động). Tối đa 02 tài khoản quản trị local dùng cho trường hợp khẩn cấp

- Sophos XG Firewall hỗ trợ các loại external svr: AD, Radius, Tacacs+, LDAP, eDirectory

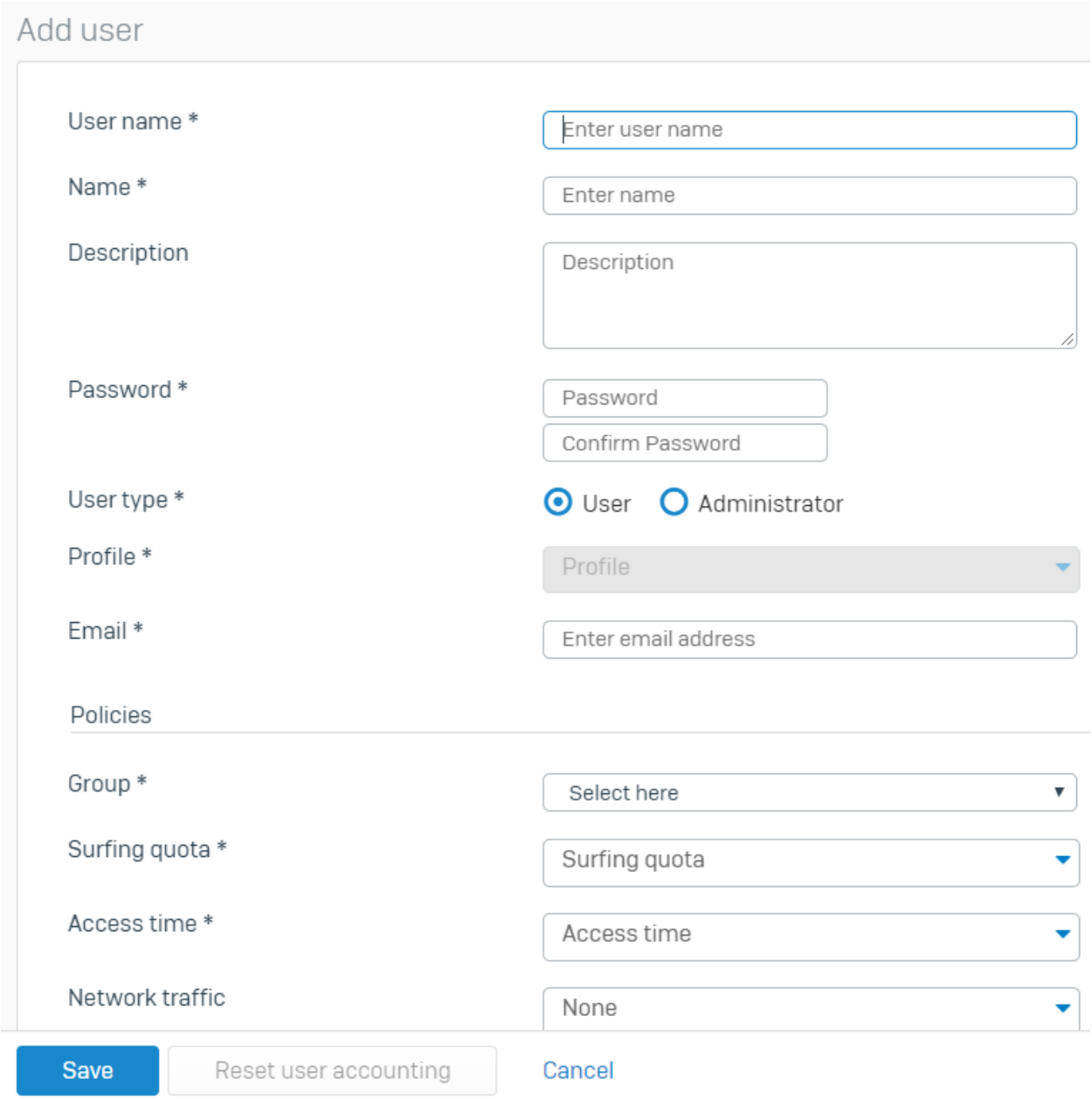
- Trên GUI:
  - Cấu hình:
    - Chọn mục **Configuration** > **Authentication** > tab **Servers** > **Add**
    - Server Type: Chọn loại Svr muốn sử dụng
    - Điền các thông tin về SVR > **Save**



- Chọn tab **Services > Administrator authentication methods**
- Tick chọn Svr AAA vừa tạo trước rồi tick chọn **Local** sau. (Ưu tiên xác thực AAA) > **Save**



- Tạo tài khoản Local: Chọn tab **Users** > click **Add**
- Nhập đầy đủ các thông tin > **Save**



- Kiểm tra: Trong mục tương tự

- Quản trị viên phải sử dụng tài khoản được cấp riêng, phân quyền phù hợp trên local/AAA

<u>Đối với tài khoản Local</u>

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Configuration** > **Authentication** > tab **Users** > click vào biểu tượng để edit user**.**
    - **Profile: Hãng định nghĩa sẵn 6 profile**

      Administrator: Full quyền

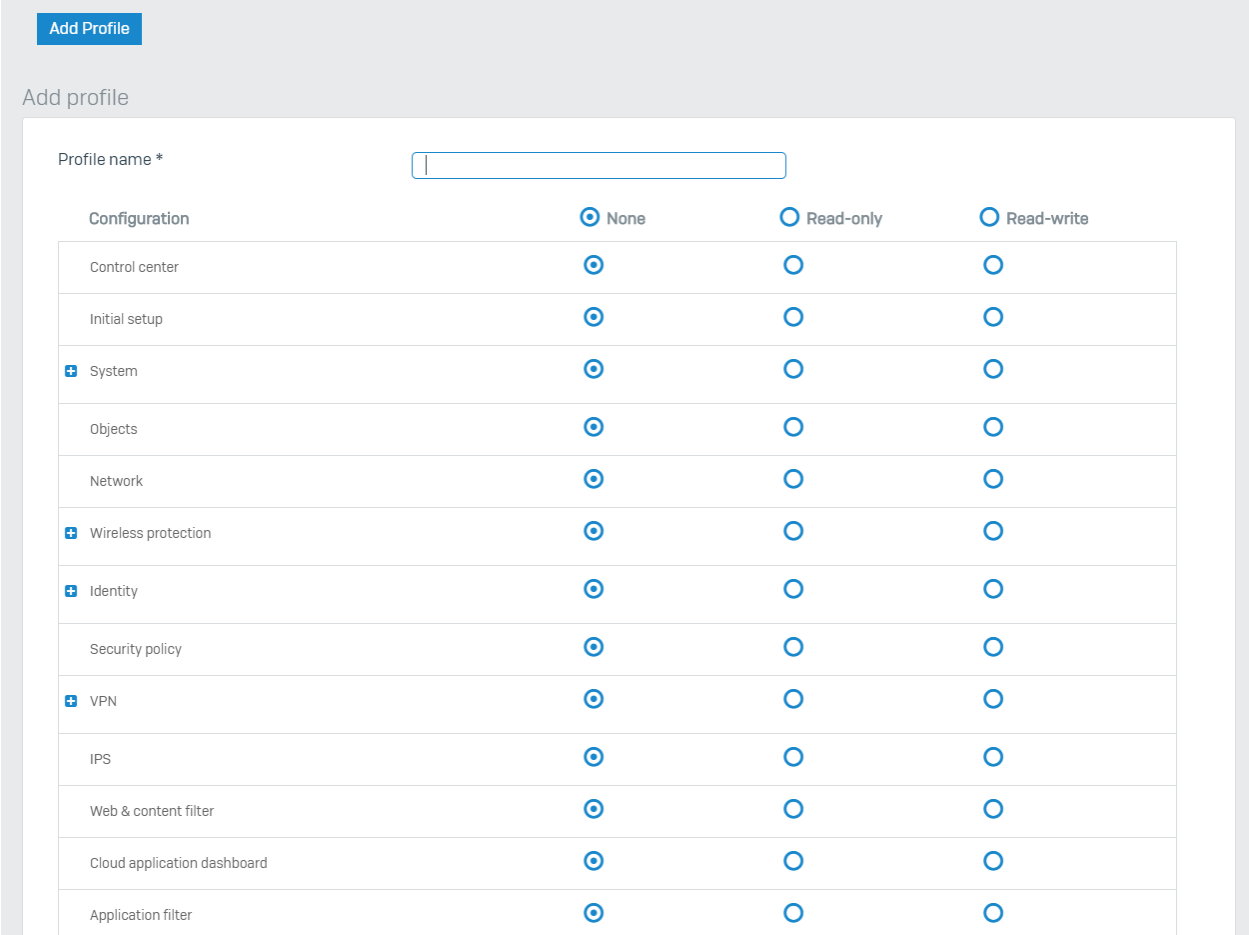
      Crypto Admin: Chỉ có quyền cấu hình CA

Security Admin: Có quyền config hầu hết các tính năng nhưng không được cấu hình, đọc Log và đổi Password

Audit Admin: Chỉ có quyền cấu hình và đọc log

HA Profile: Có quyền view đầy đủ. Được cấu hình HA, Lisence và reboot thiết bị

Có thể sử dụng các profile có sẵn ở trên hoặc tạo profile theo ý muốn > click **Create New**



- **Chọn các quyền theo ý muốn > Save**
- Click **Save**

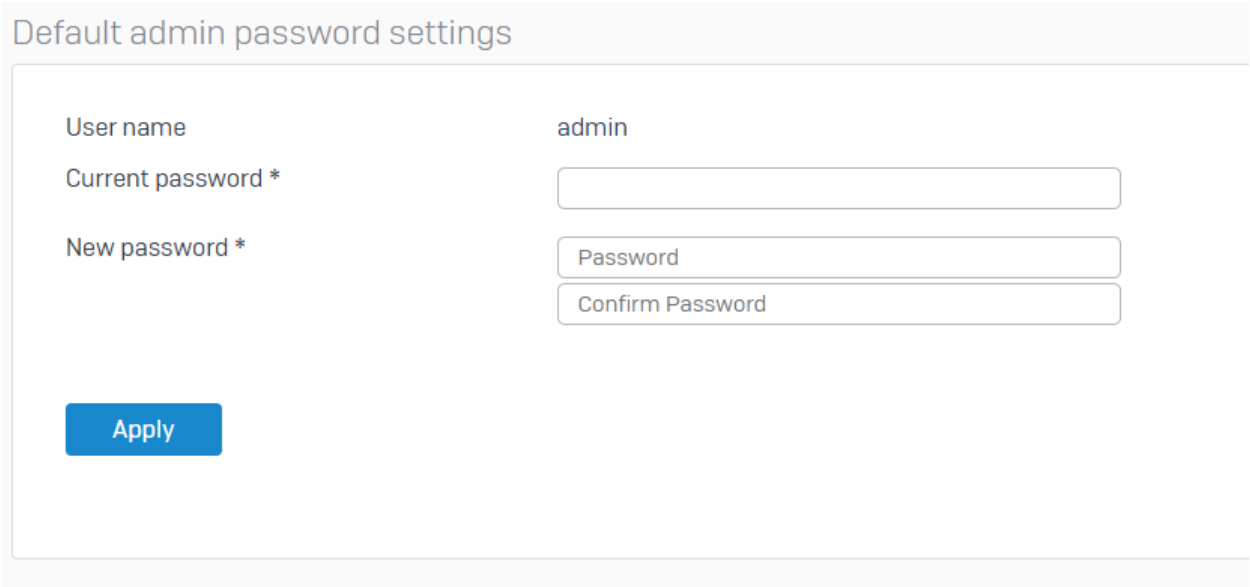
- Kiểm tra: Trong mục tương tự

<u>Đối với tài khoản AAA</u>

- Kiểm tra trực tiếp chính sách trên máy chủ AAA

- Đổi mật khẩu mặc định các tài khoản local của thiết bị

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Administration > Device Access> Default admin password settings** > Đổi pass> **Apply**

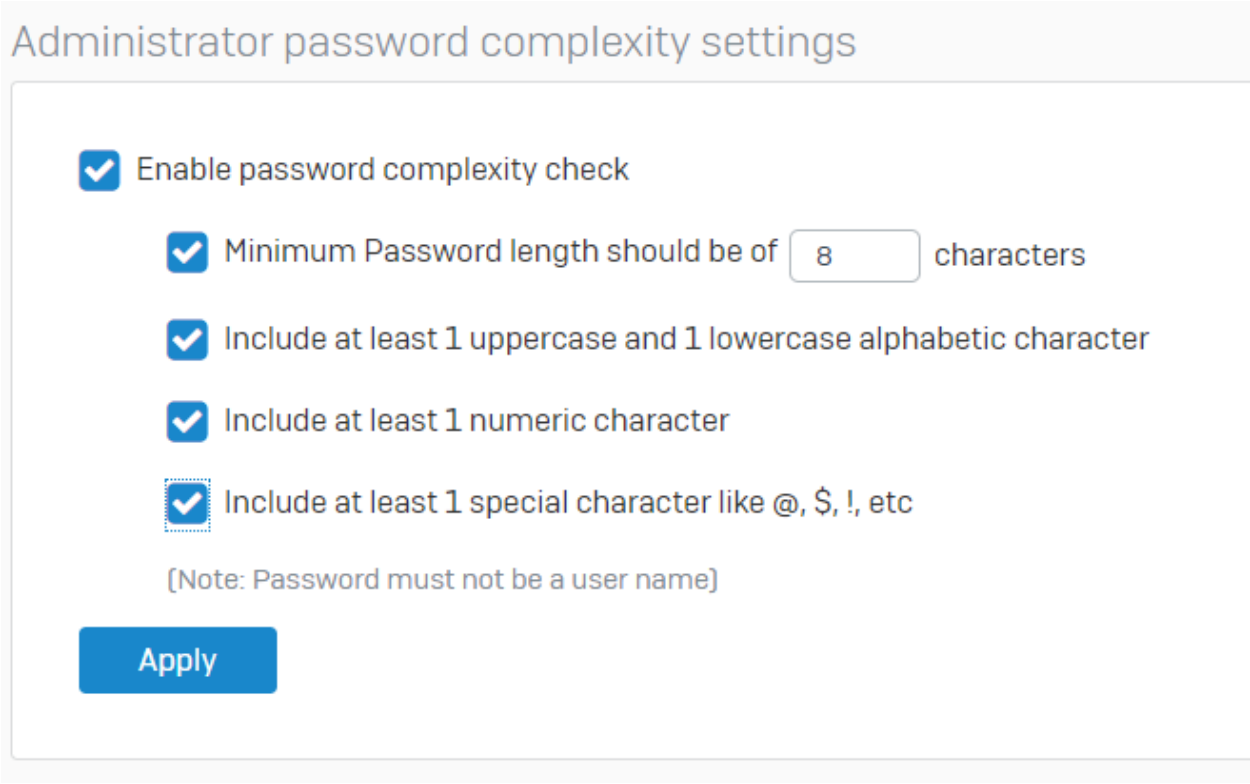


- Kiểm tra: Login lại acc admin

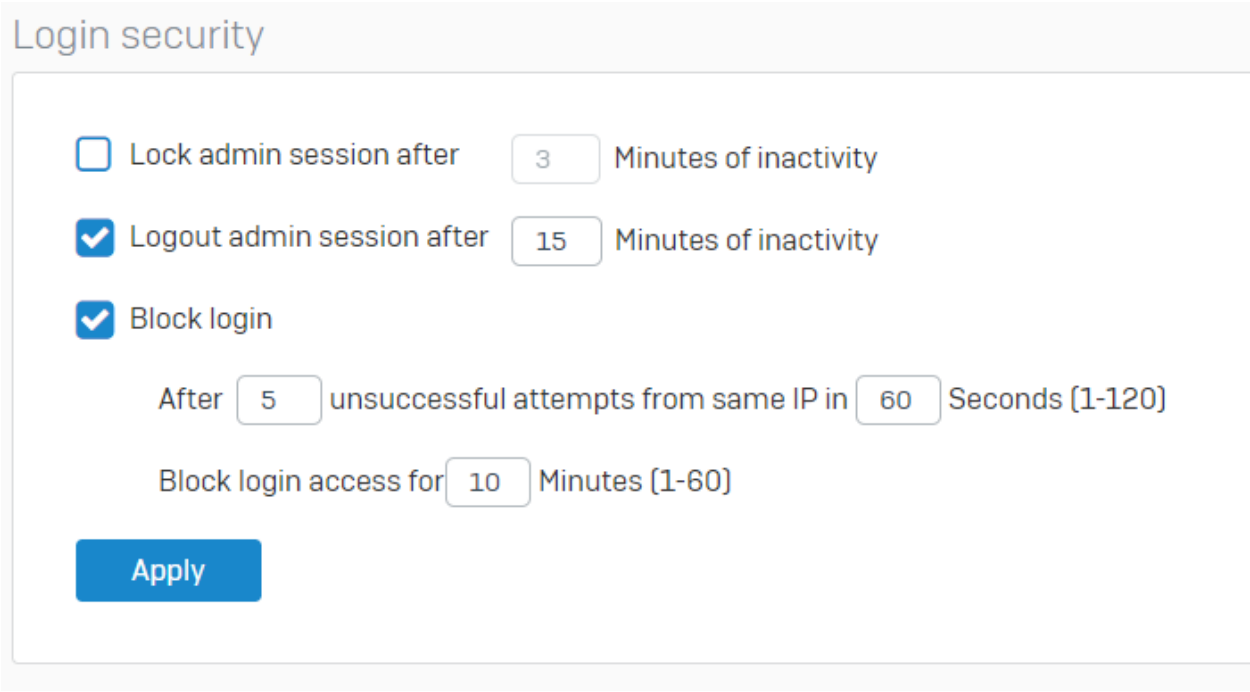
- Thiết lập chính sách mật khẩu mạnh cho các tài khoản trên local/AAA. Khóa sau 5 lần đăng nhập sai, thời gian khóa tài khoản do đăng nhập sai là 10 phút

Đối với account local

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Administration > Admin Settings> Administrator password complexity settings** > Tick chọn tất cả các options > **Apply**



- Chọn mục **Login security** > Tick chọn như hình dưới > **Apply**



- Kiểm tra: Trong mục tương tự

Đối với account AAA

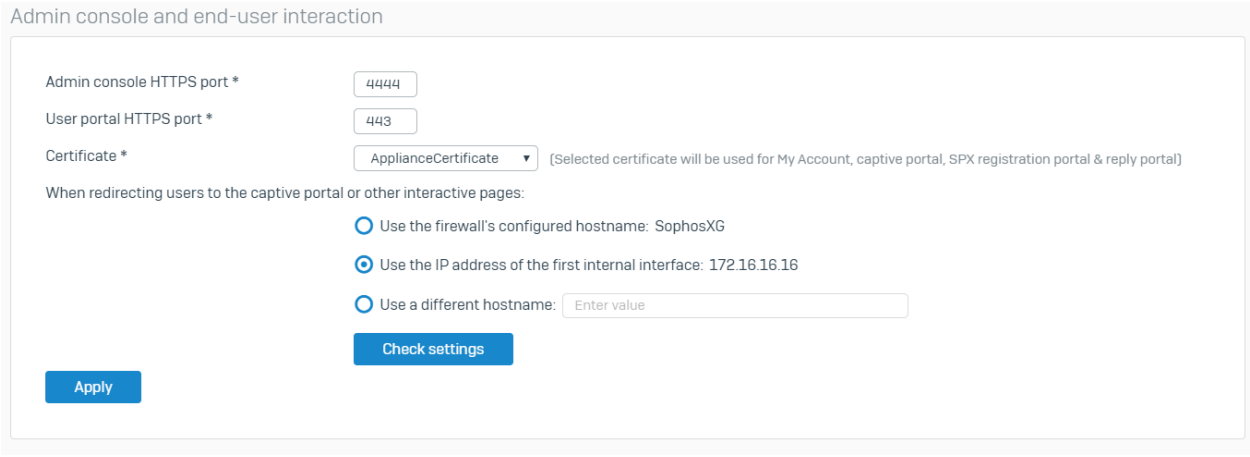
- Kiểm tra trực tiếp chính sách trên máy chủ AAA

4.3. Yêu cầu về kết nối quản trị

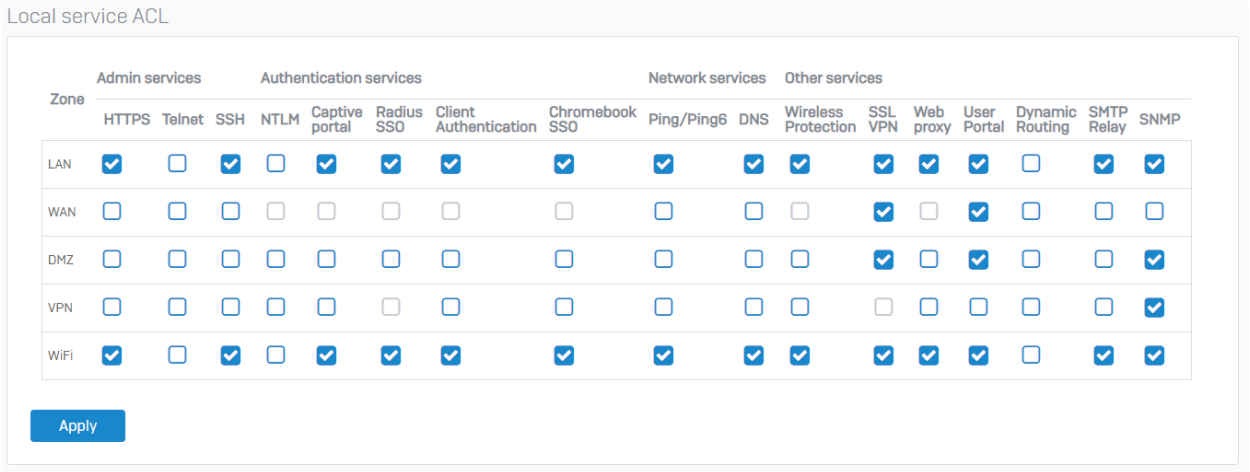
- Quản trị thiết bị qua VLAN quản trị dành riêng.
  - Kiểm tra trên cấu hình, đấu nối IP, quy hoạch VLAN quản trị

- Quản trị thiết bị qua kết nối trực tiếp Console hoặc kết nối từ xa an toàn, có mã hóa (SSHv2, HTTPS). Tắt các giao thức quản trị từ xa không an toàn (Telnet, HTTP)

  - Trên GUI:
    - Cấu hình:
      - Mặc định các kết nối HTTP được redirect sang HTTPS
      - Cấu hình port cho các kết nối HTTPS: chọn mục **System > Administration > Admin Settings > Admin console and end-user interaction > Apply**



      - Chọn mục **System > Administration > Device Access> Local service ACL > bỏ tick ở cột Telnet > Apply**

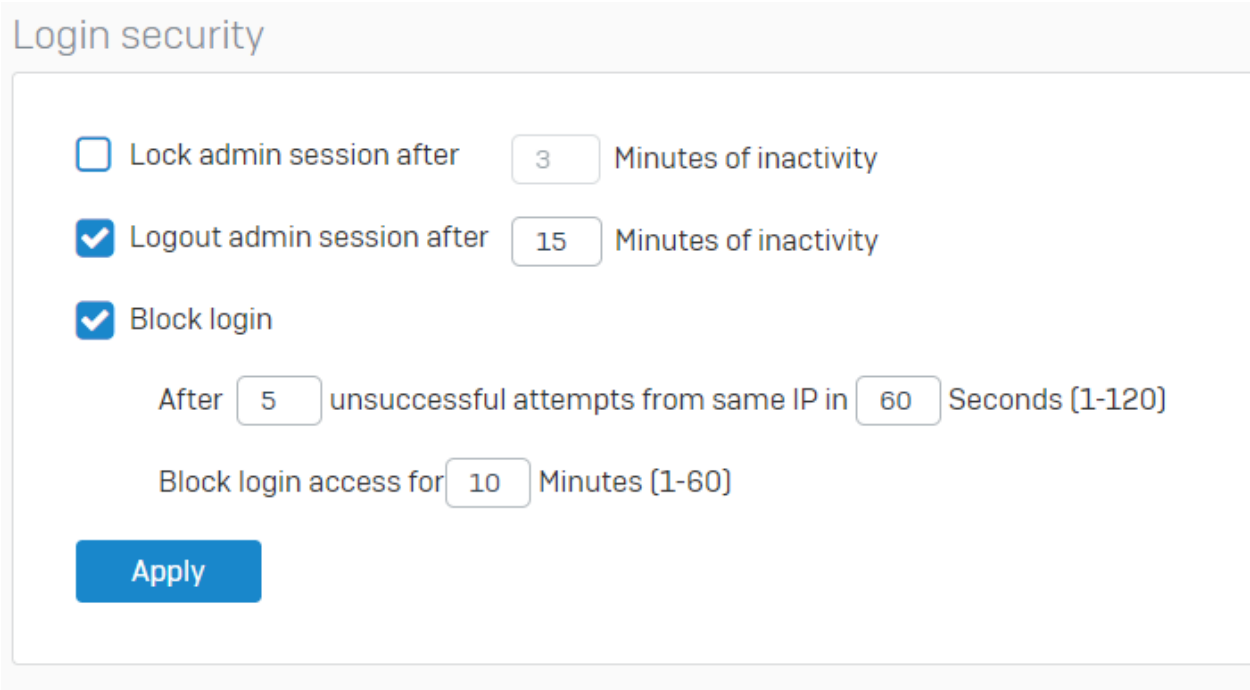


    - Kiểm tra: Thử kết nối quản trị bằng telnet và http

- Thời gian time-out của các phiên kết nối quản trị tối đa là 15 phút

  - Trên GUI:
    - Cấu hình:
      - Chọn mục **System > Administration > Admin Settings > Login security.**

- Tick chọn **Logout admin session after** và nhập giá trị **15**



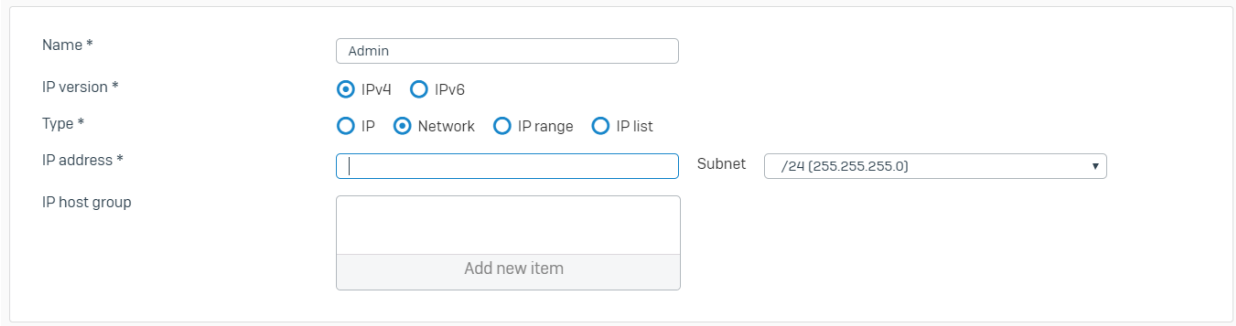
- Kiểm tra: Trong mục tương tự

- Giới hạn chỉ cho phép quản trị từ các IP theo danh sách đăng kí

- Trên GUI:

- Cấu hình:

- Chọn mục **System > Host and Services > IP host > Add**
- **Điền IP hoặc dải IP quản trị > Save**



- Chọn mục **System > Administration > Device Access> Local service ACL > Local service ACL exception rule** > Click **Add.** Điền các thông số như dưới > **Save**

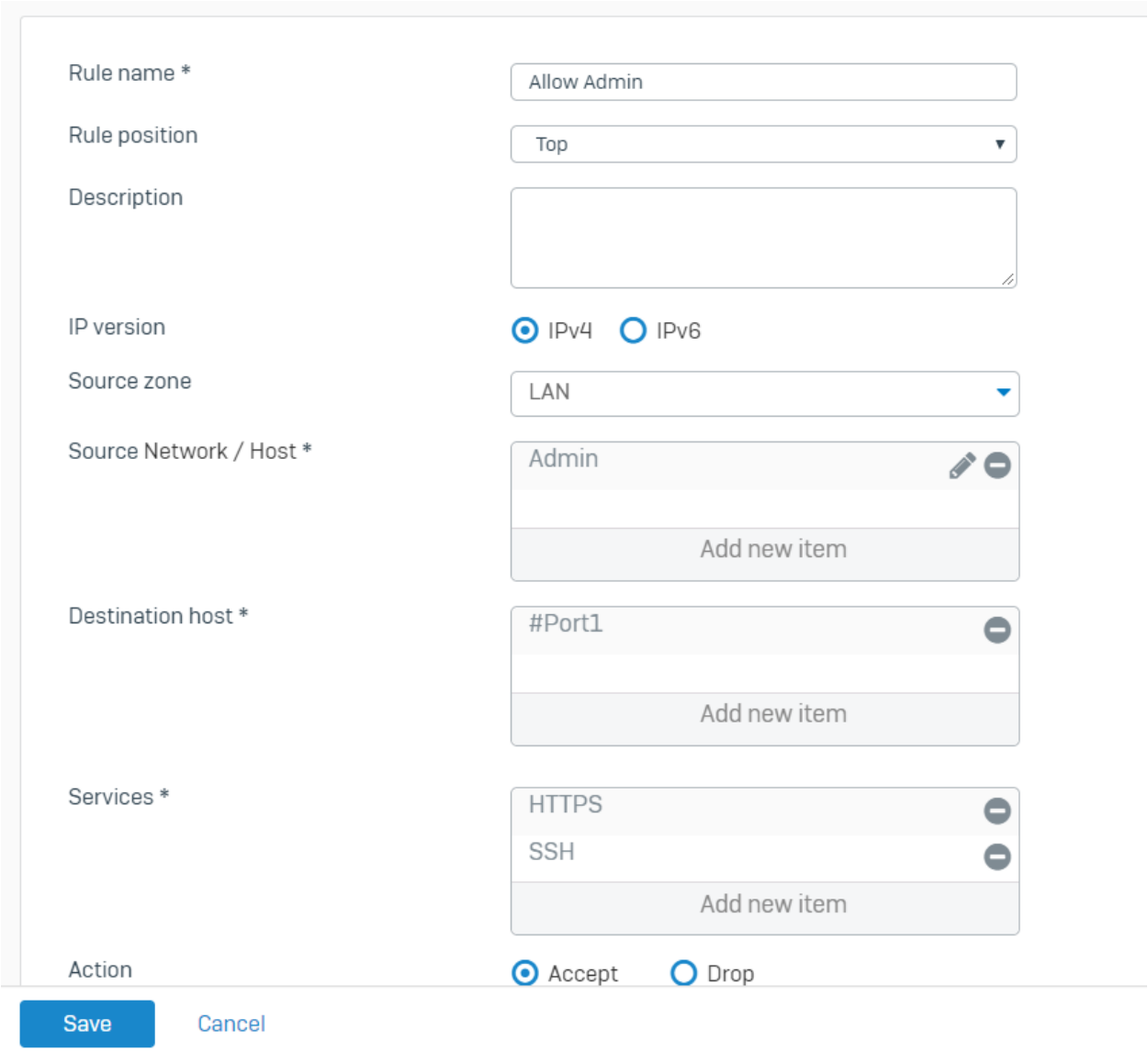
  Source Zone: Chọn Zone của người dùng quản trị

  Source Network: Chọn danh sách IP admin vừa tạo ở trên

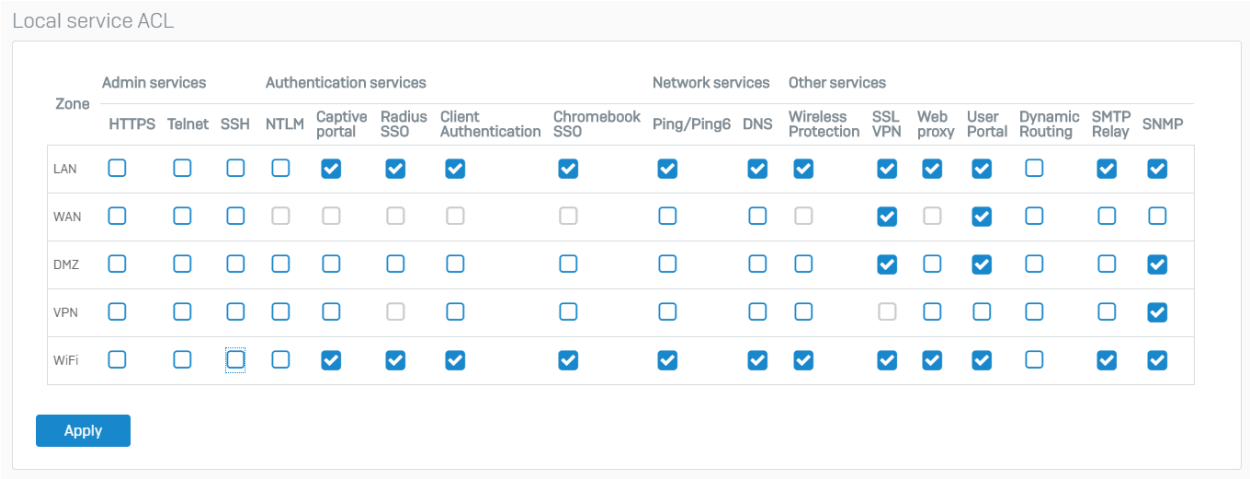
  Destination Host: Chọn Interface kết nối quản trị đến

  Service: Tick chọn **https** và **ssh**

  Action: Tick chọn **Accept**



- Trong **Local service ACL**, bỏ tick ở cột **HTTPS** và **SSH** > **Apply**

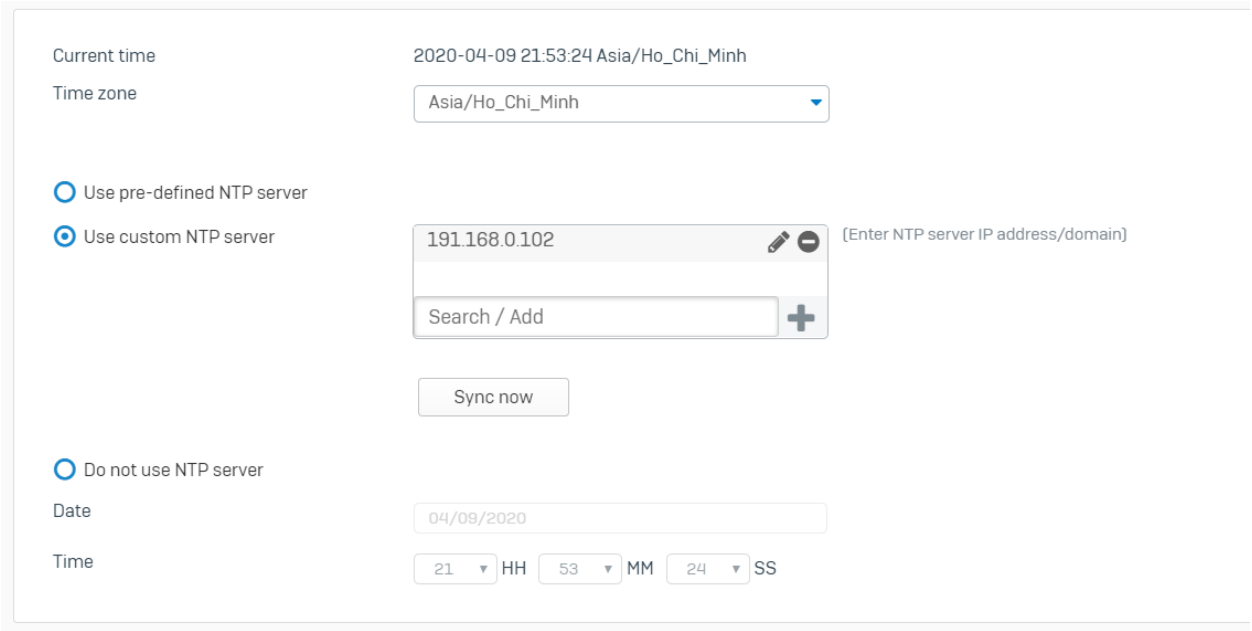


- Kiểm tra: Trong mục tương tự

4.4. Yêu cầu cấu hình NTP

- Thiết bị phải được đồng bộ thời gian theo tối thiểu 01 máy chủ thời gian (NTP server)

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Administration > Time**
    - Time Zone chọn Asia/Ho_Chi_Minh
    - Tick chọn **use custom NTP server** > nhập IP NTP server > click vào biểu tượng **> Sync Now > Apply**

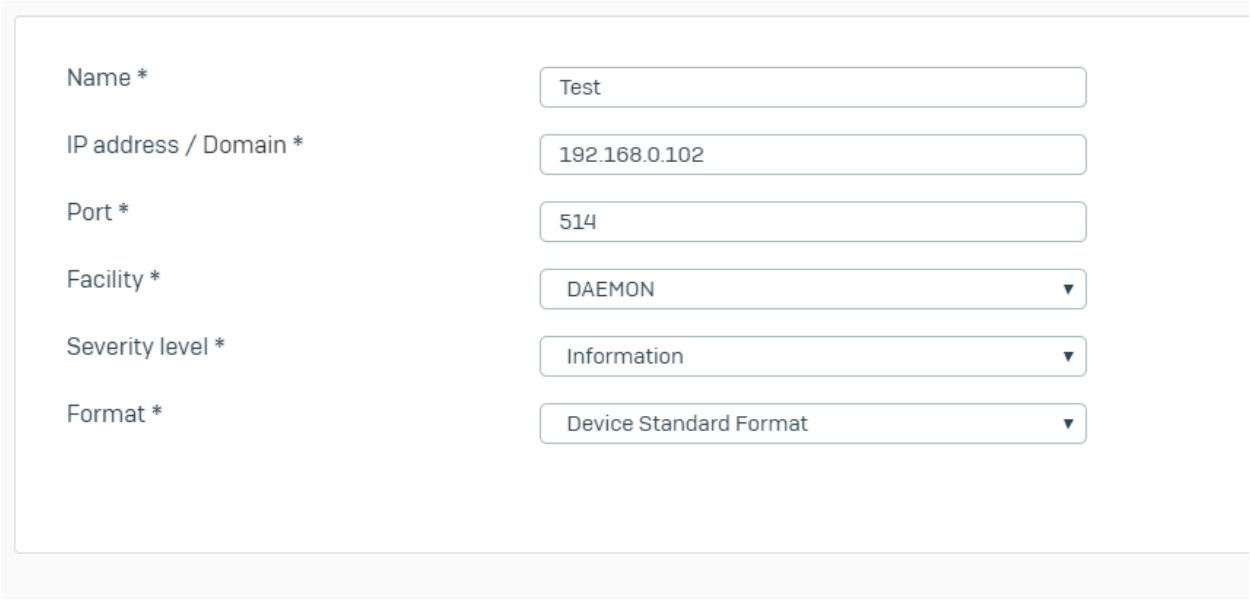


  - Kiểm tra: Trong mục tương tự

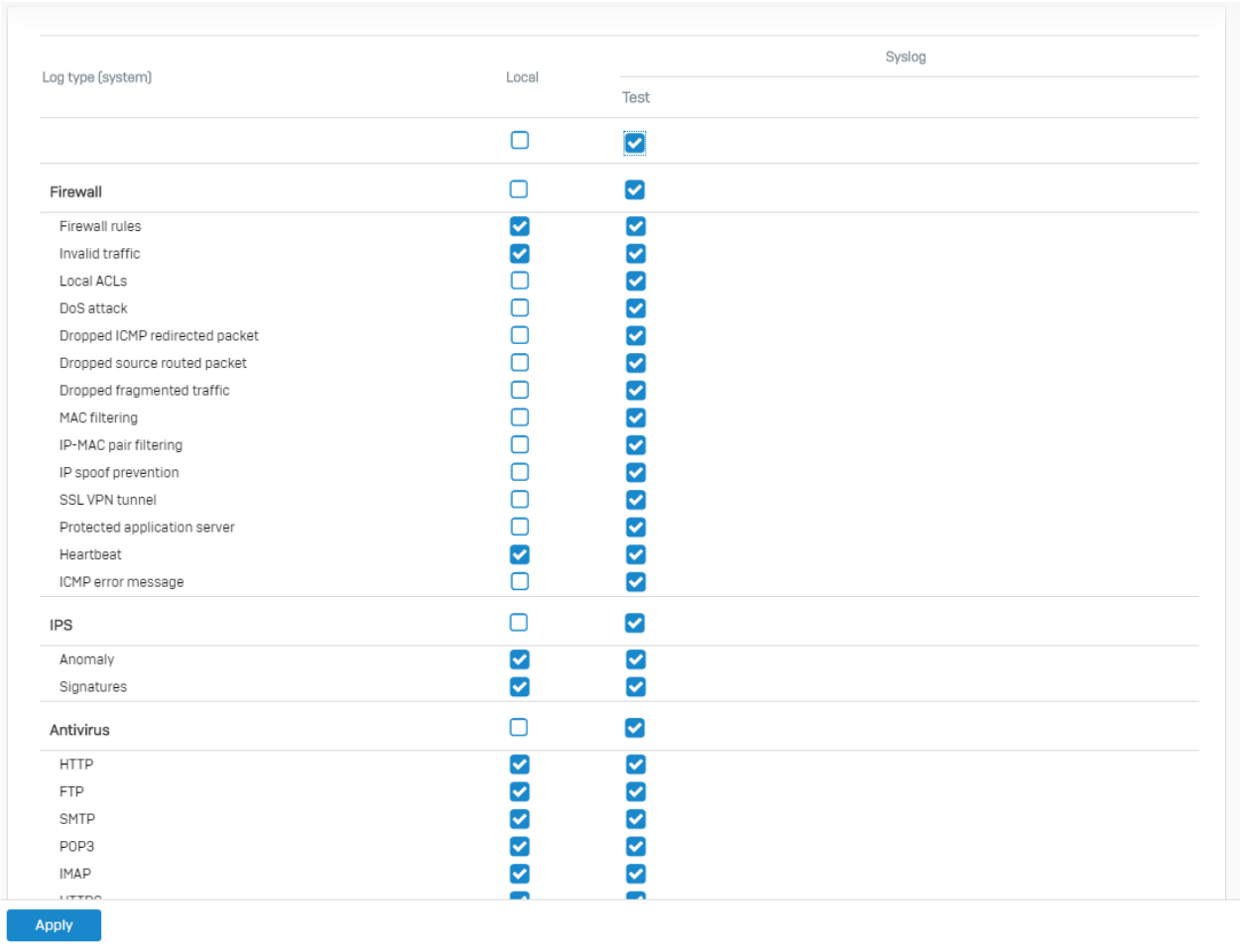
4.5. Yêu cầu cấu hình log

- Thiết bị phải được thiết lập bật chế độ ghi log và cấu hình lưu log tập trung tối thiểu 06 tháng. Trong trường hợp không có hệ thống lưu log tập trung thực hiện thiết lập lưu trên local

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Configuration > System Services > Log Settings > Syslog Servers > Add**
    - Nhập các thông số cho svr. **Severity** chọn **Warning**



- Chọn mục **tab Log Settings** > Ở cột Syslog tick chọn các loại log cần lấy > **Apply**



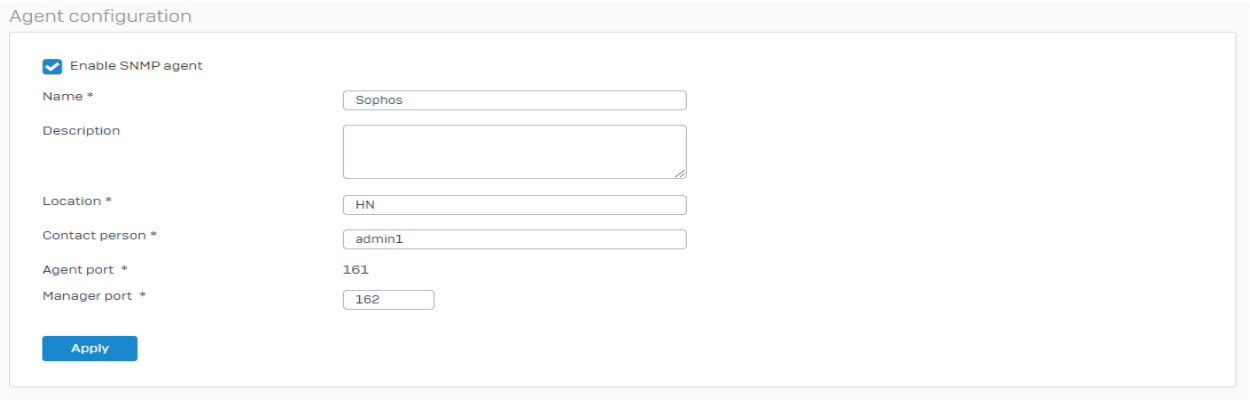
  - Kiểm tra: Trong mục tương tự

4.6. Yêu cầu cấu hình SNMP

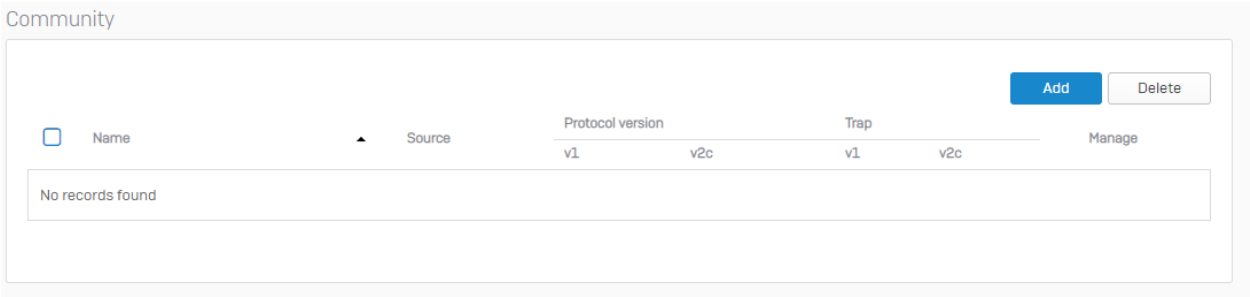
- SNMP phiên bản v2c, v3. SNMP theo chế độ read-only. Community string SNMP riêng. Xóa bỏ community string mặc định. Chỉ cho phép truy cập SNMP từ máy chủ giám sát.

- Sophos XG Firewall chỉ hỗ trợ SNMP V2c

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Administration > SNMP > Agent configuration**



    - Tick chọn **Enable SNMP agent** > Điền các thông số cho Agent > **Apply**
    - Trong **Community** - click **Add**



    - Điền các thông tin > **Save**

      Name: Community String

      IP address: Ip của SNMP Manager

      Protocol: Chọn V2c

      Trap support: Chọn V2c

- Kiểm tra: trong mục tương tự

5. Thiết lập các tính năng an ninh

5.1. Yêu cầu bật tính năng phòng chống tấn công mạng trên các Firewall

- Bật và cấu hình các tính năng phòng chống tấn công mạng phù hợp với hệ thống CNTT được Firewall bảo vệ (IPS/IDS, UTM, Screening)

Đối với IPS/IDS: (*Intrusion prevention*)

- Cấu hình:
  - Sophos cung cấp sẵn 10 IPS/IDS policies. Mỗi policy gồm tập các attack signatures đã được phát hiện và các actions cần thiết tương ứng.
  - Các policies gồm:

    1. DMZ TO LAN
    2. DMZ TO WAN
    3. LAN TO DMZ
    4. LAN TO WAN
    5. WAN TO DMZ
    6. WAN TO LAN
    7. General policy
    8. lantowan strict policy
    9. lantowan general policy
    10. DMZpolicy

    Trong đó 1-6 là các policies không thể chỉnh sửa và 7-10 là các policies có thể tùy chỉnh theo nhu cầu.
  - Các action khi match signature theo 2 kiểu là packet-based và Session-based:

    Allow Packet: Cho phép packet đến đích.

    Drop Packet: Drops packets if detects any traffic that matches the signature.

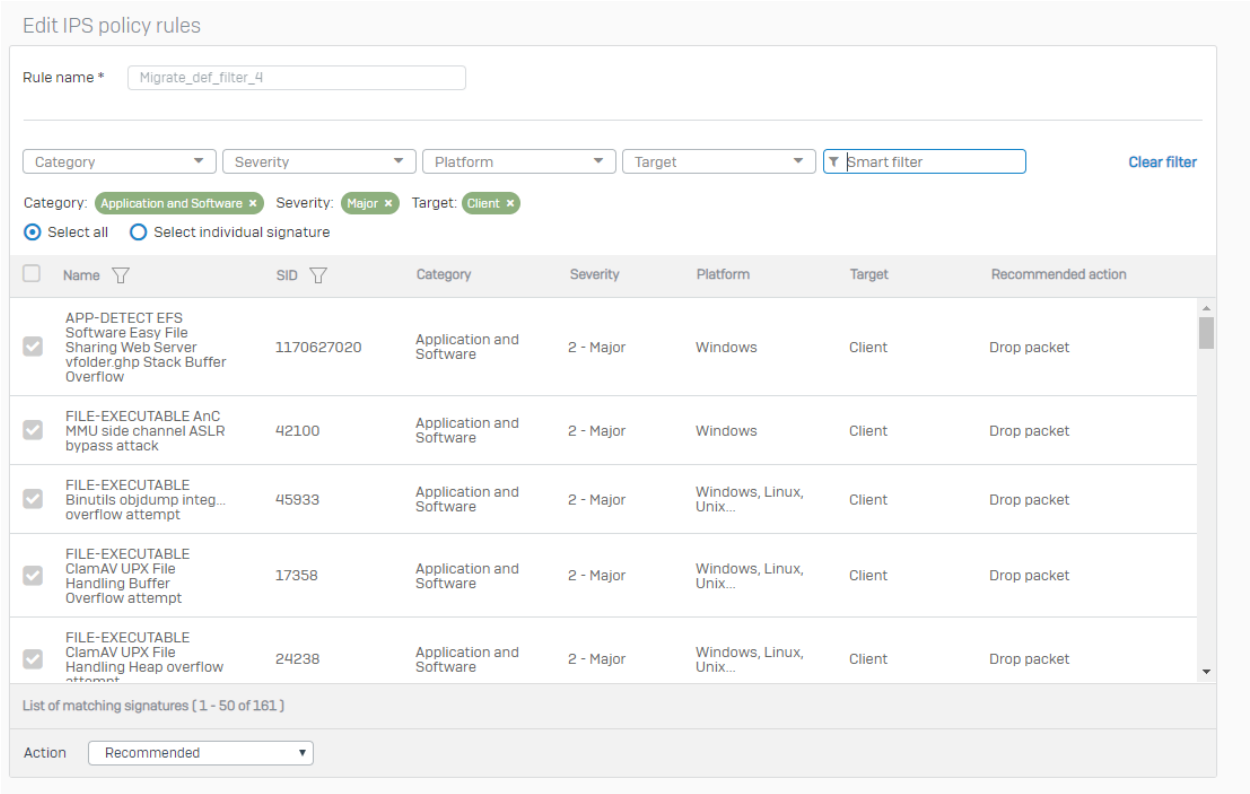
    Disable: Disables signature

    Drop Session: Drops toàn bộ session

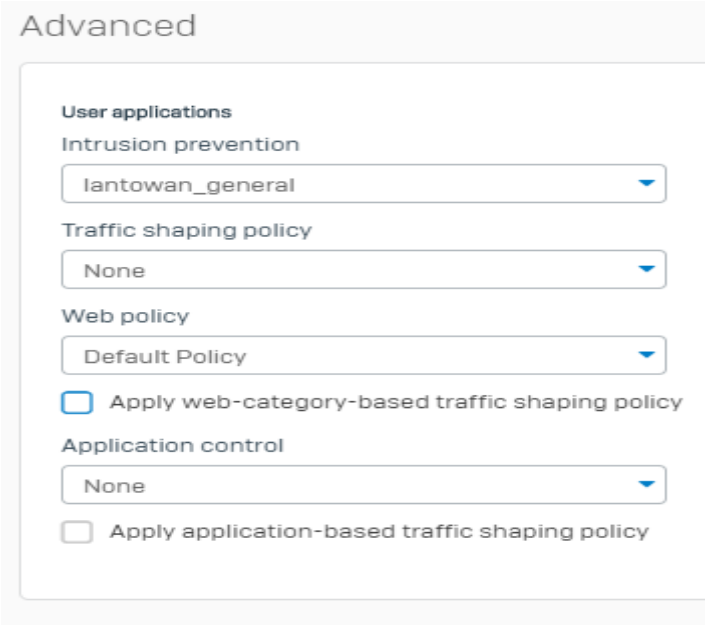
    Reset: Bắn TCP-reset đến cả client và svr

Bypass Session: Cho phép session.

- Kiểm tra và chỉnh sửa Policy.
  - Chọn mục **Protect > Intrusion Prevention > IPS/IDS policies** > click vào biểu tượng trong policy cần kiểm tra và chỉnh sửa > Click vào Rule cần xem



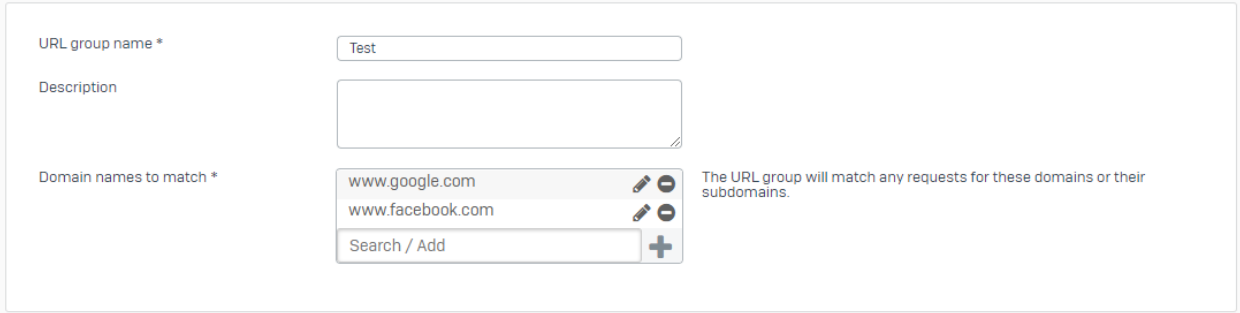
  - Để thêm signature click **Category** và tick chọn các Category Signature mong muốn. Click vào **action** để chỉnh sửa action > **Save**
- Enable IPS/IDS trên Firewall Policy
  - Chọn mục **Protect > Firewall** > click chọn Policy cần enable IPS/IDS.
  - Trong **Advanced > Intrusion Prevention** chọn IPS/IDS policy phù hợp > **Save**



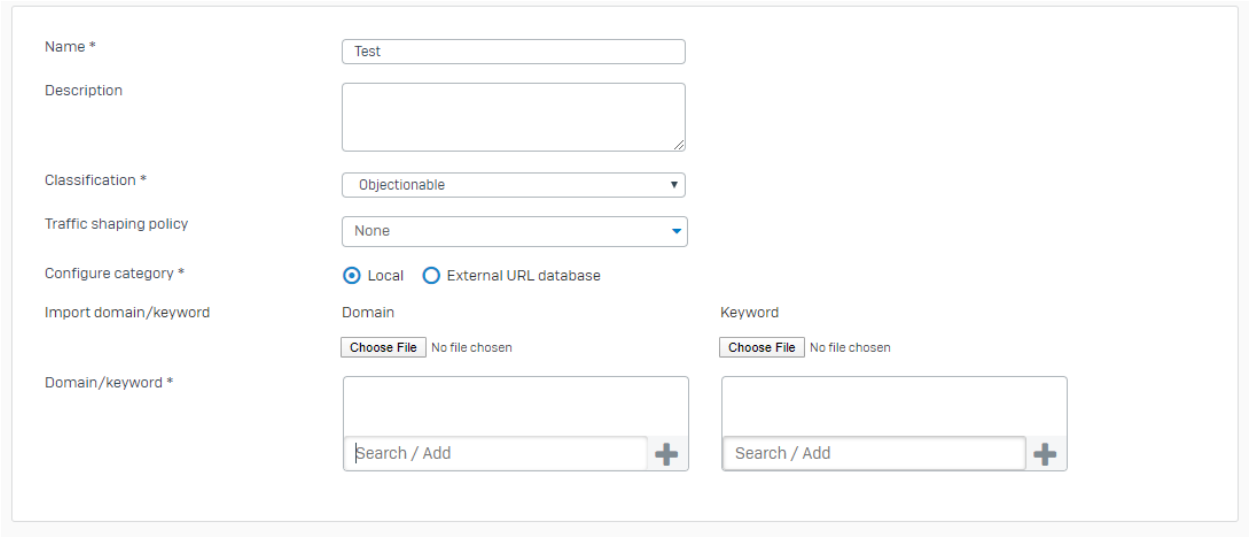
- Kiểm tra: Trong mục tương tự

<u>Đối với URL-filtering(Web)</u>

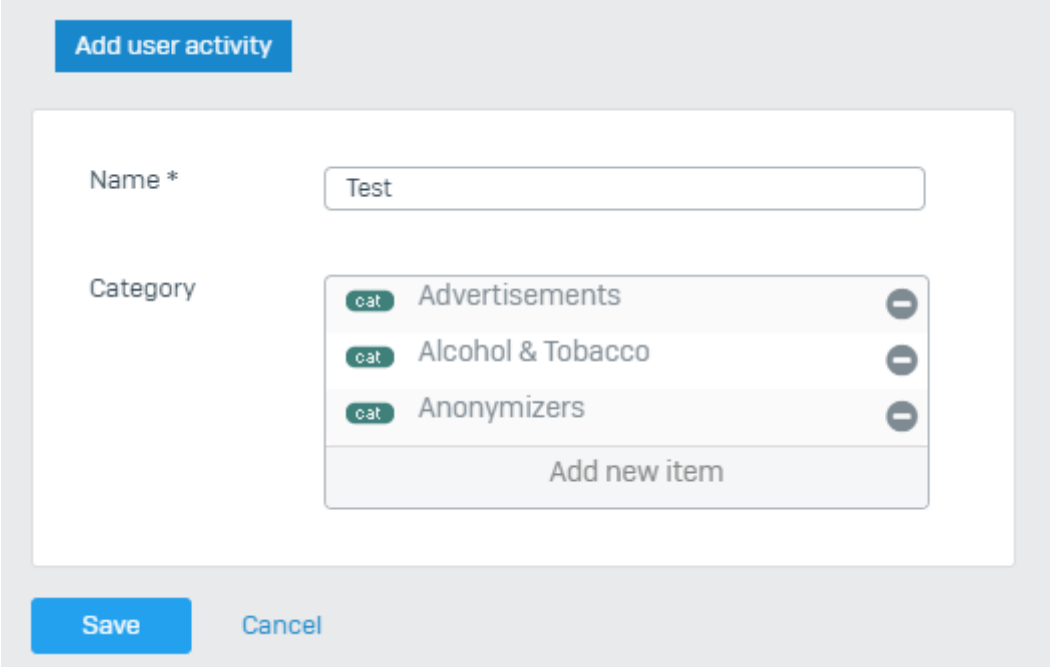
- Sophos cung cấp sẵn 1 số các Web policies. Mỗi policy gồm tập các Rule. Mỗi Rule bao gồm các User Activities và action tương ứng. Mỗi Activities chứa các Categories Web, URL group (User define) và các loại file có thể download.
- Cấu hình:
  - Tạo URL group:
    - Chọn mục **Protect > Web > URL group > Add**
    - Domain names to match: Nhập các URL theo nhu cầu > click vào biểu tượng để add URL > **SAVE**



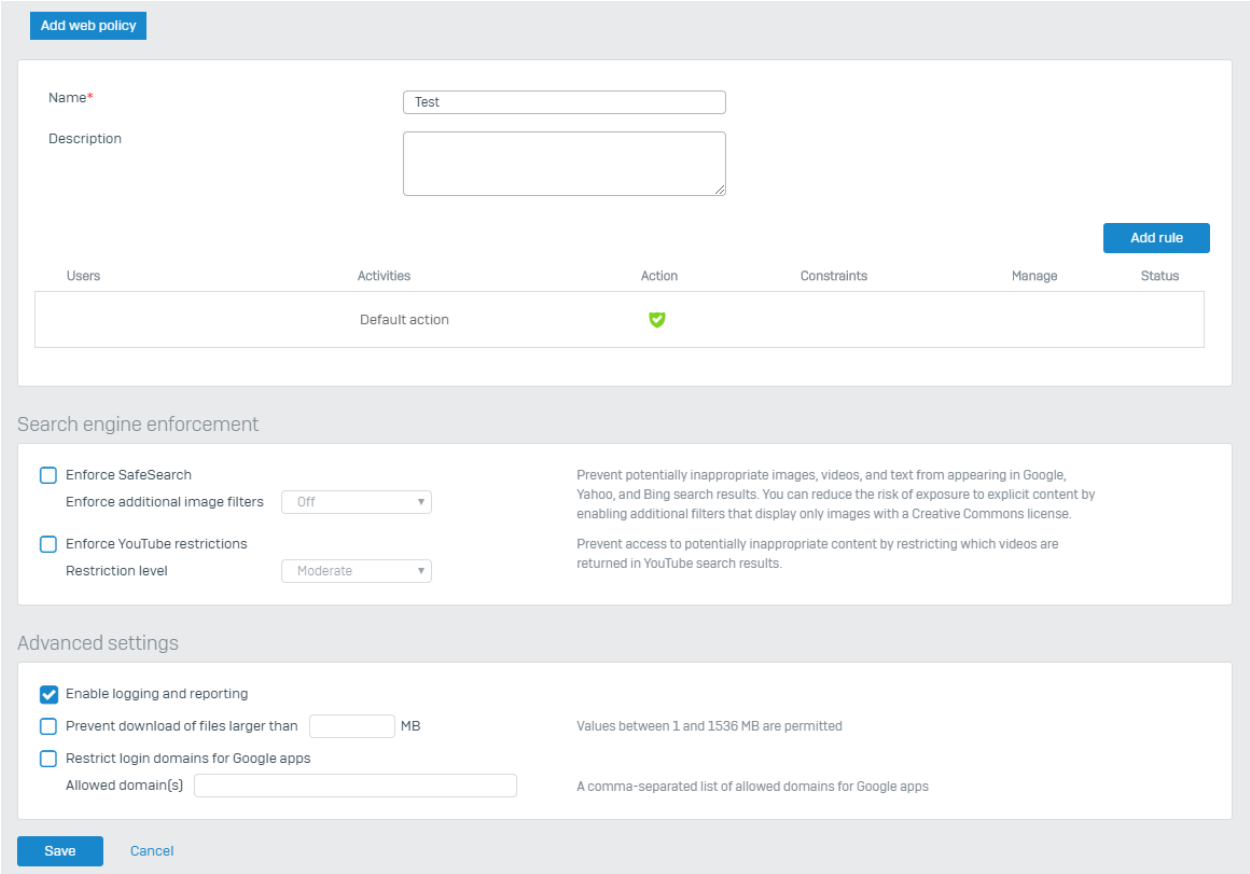
  - Tạo Categories:
    - Chọn mục **Protect > Web > Categories > Add**
    - Có thể Import các file chứa Domain/keyword (hỗ trợ các kiểu file .txt, .gz, .tar, .bz và .bz2) hoặc add thủ công > **Save**



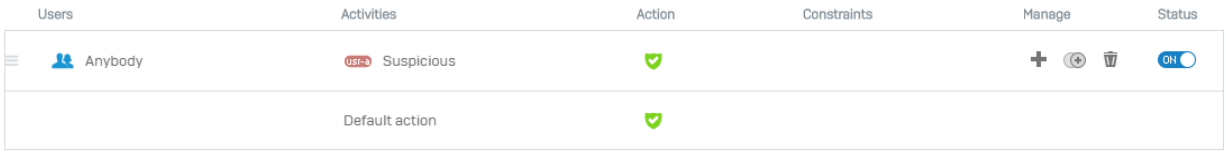
- Tạo User Activities:
  - Chọn mục **Protect > Web > User Activities > Add**
  - Trong Category > Click Add new item > Tick chọn các Categories, URL group, File trong danh sách > **Save**



- Tạo Web Policies:
  - Chọn mục **Protect > Web > Policies > Add Policy**



- Click **Add Rule**



- Chọn các thông tin theo nhu cầu > **Save**

  Users: Chọn các user hoặc group ảnh hưởng

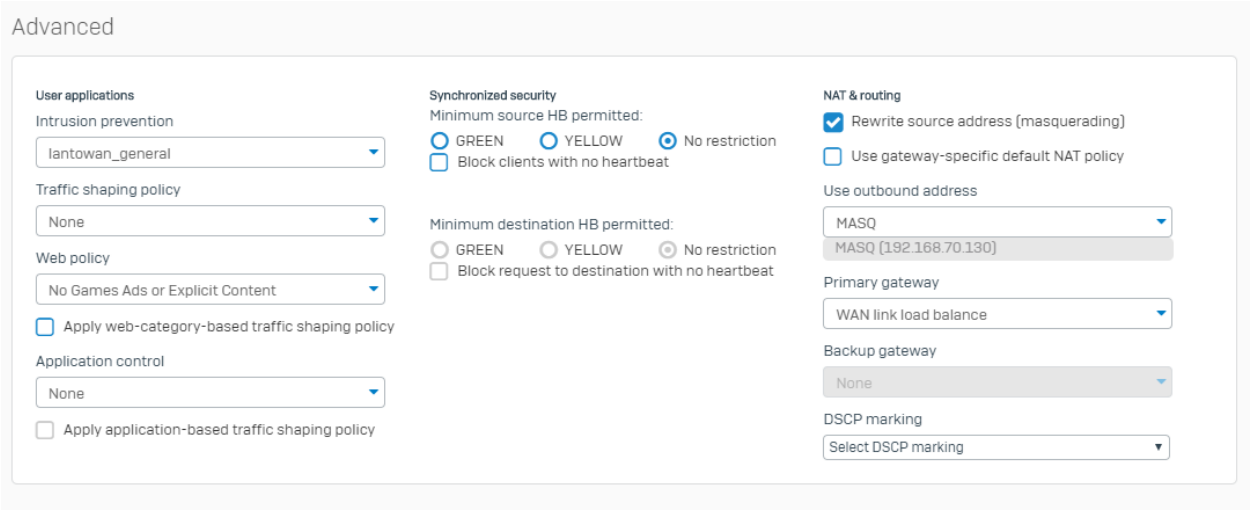
  Activities: Chọn các Activities, Categories, URL-group, File Type vừa tạo hoặc hãng tạo sẵn.

  Action: Allow, Warning và Block

  Constraints: thời gian hiệu lực của Rule

  Status: Switch sang ON

- Apply vào Firewall Policy:
  - Chọn mục **Protect > Firewall >** chọn Policy cần thêm Web-filter
  - Trong **Web policy**: chọn Policy vừa tạo > **Save**



- Kiểm tra: Trong mục tương tự

5.2. Yêu cầu rule phát hiện và ngăn chặn các kết nối C&C

- Khai báo phát hiện và ngăn chặn các kết nối C&C, các domain độc hại. Khai báo rule ở vị trí có hiệu lực đầu tiên

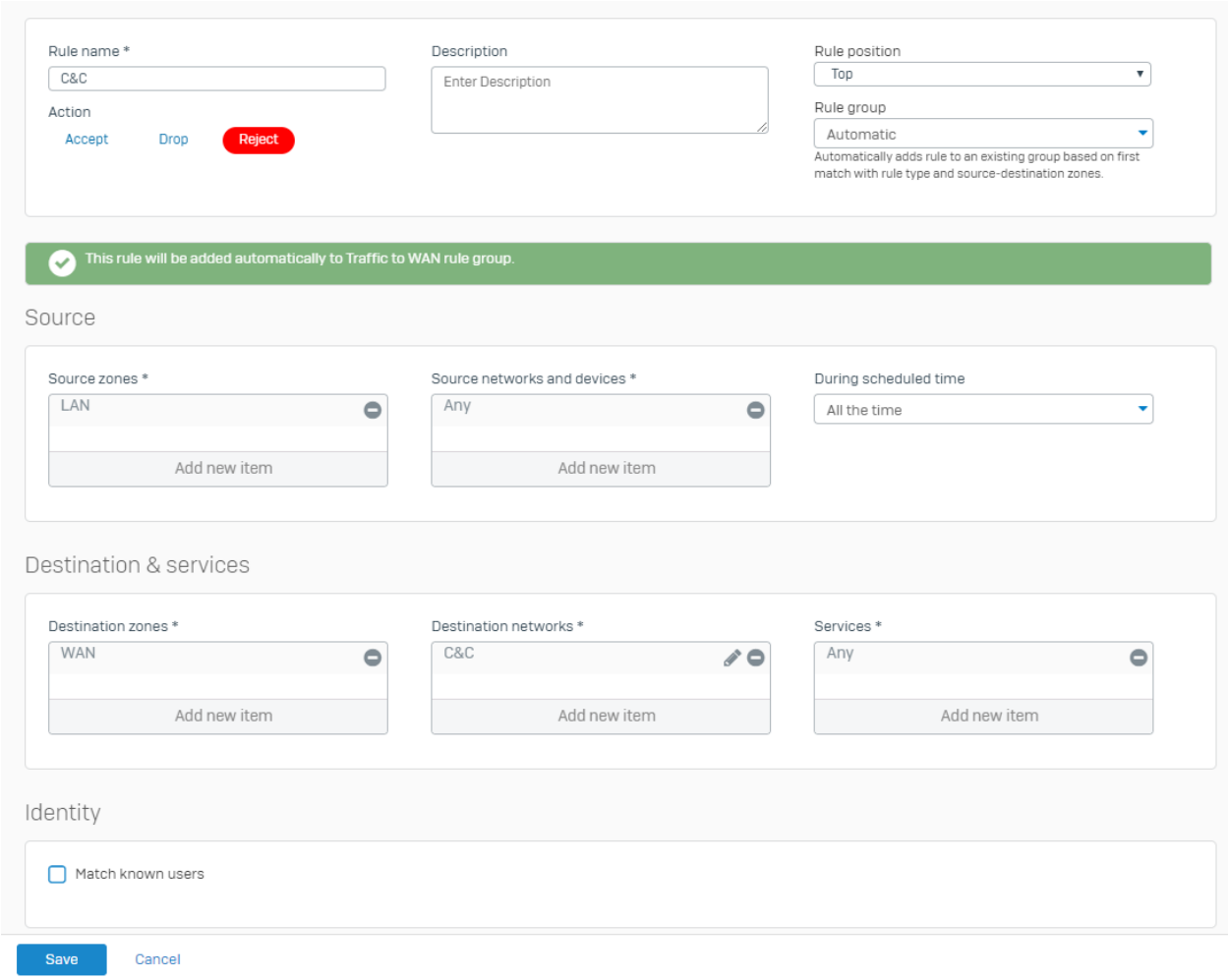
- Cấu hình
  - Chọn mục **Protect > Firewall > Add Firewall Rule > User/Network Rule**
  - Chọn các thông tin như sau:

    Rule position: Chọn Top

    Action: Chọn Reject

    Source Zone là Trusted Zone, source network là any

    Destination Zone là Untrusted Zone, Destination network là list IP C&C.
  - Tick chọn **Log firewall traffic > Save**



- Kiểm tra: Trong mục tương tự

5.3. Yêu cầu rule phát hiện và chặn người dùng quản trị ra Internet

- Khai báo rule phát hiện và chặn người dùng quản trị ra Internet trực tiếp và qua Proxy, chỉ mở cho người dùng quản trị đến các hệ thống theo các port quản trị TCP-22 (SSH), (TCP-23 (Telnet), TCP-3389 (RDP),1433 (MS-SQL), TCP-1521->1527 (Oracle), TCP-3306 (Mysql), TCP-5432 (postgresql), TCP/UDP-161/162 (SMTP)

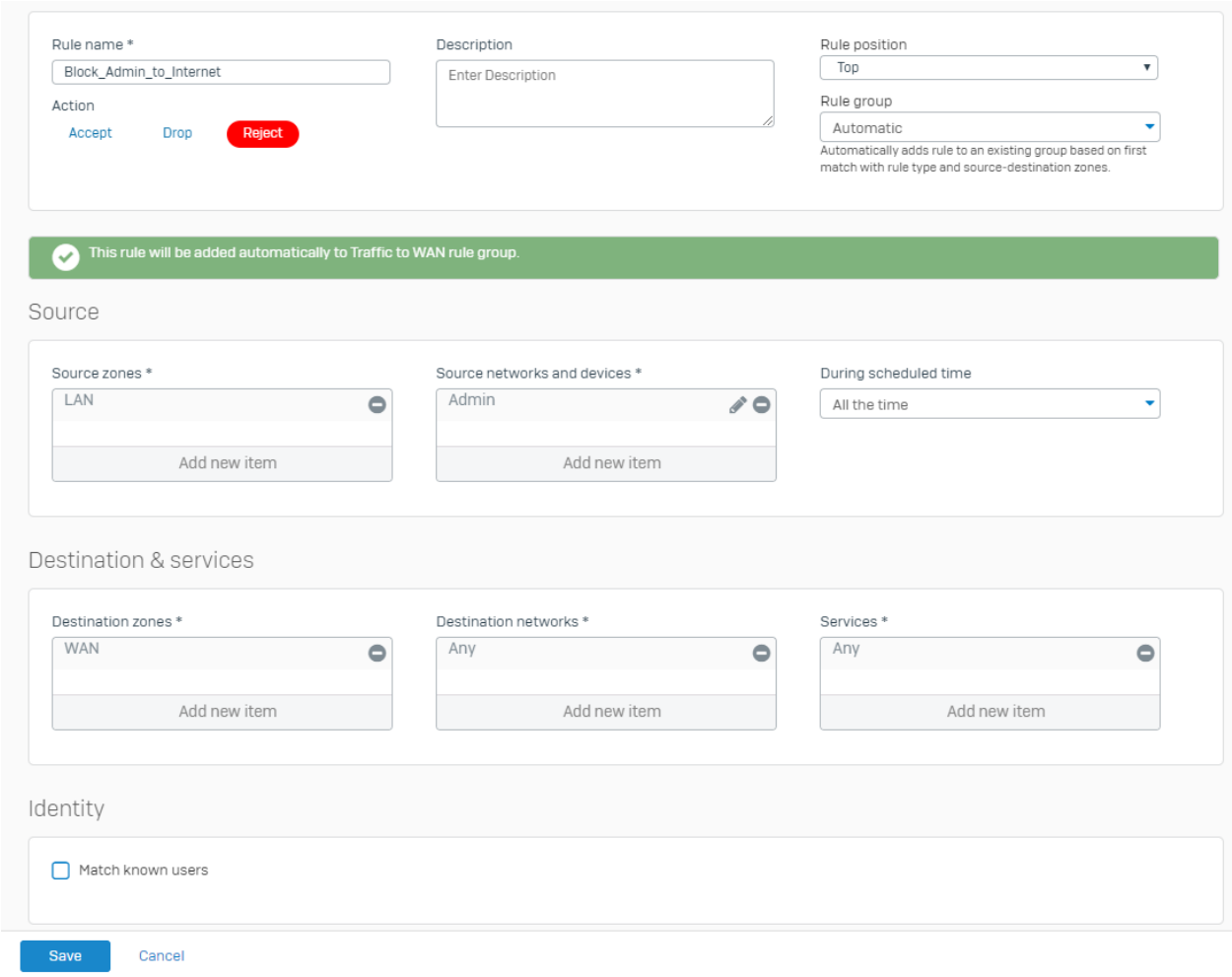
- Cấu hình
  - Chọn mục **Protect > Firewall > Add Firewall Rule > User/Network Rule**
  - Chọn các thông tin như sau:

    Rule position: Chọn Top

    Action: Chọn Reject

    Source Zone là Trusted Zone, source network là dải IP quản trị

    Destination Zone là Untrusted Zone, Destination network là any.
  - Tick chọn **Log firewall traffic > Save**



- Kiểm tra: Trong mục tương tự

5.4. Yêu cầu rule phát hiện và chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao

- Khai báo rule phát hiện và chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao:

- Internet: Level 1
- Wan: Level 2
- Office: Level 3
- DMZ: Level 4
- Server Farm: Level 5
- Cấu hình

  - Chọn mục **Protect > Firewall > Add Firewall Rule > User/Network Rule**
  - Chọn các thông tin như sau:

    Rule position: Chọn Top

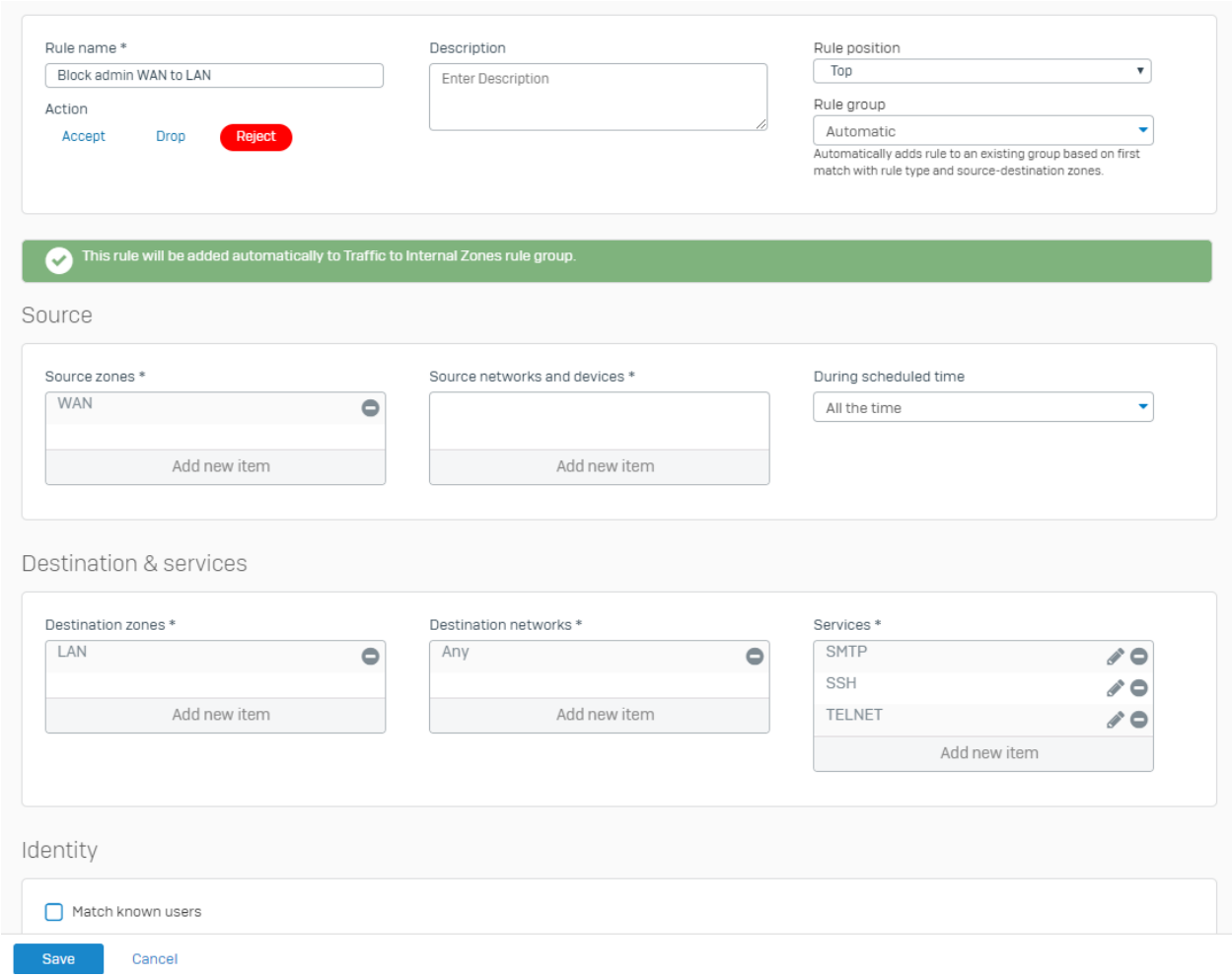
Action: Chọn Reject

Source Zone là các zone security level thấp, source network là any

Destination Zone là các zone security level cao, destination network là any

Service: Chọn các port quản trị TCP-22 (SSH), (TCP-23 (Telnet), TCP-3389 (RDP),1433 (MS-SQL), TCP-1521->1527 (Oracle), TCP-3306 (Mysql), TCP-5432 (postgresql), TCP/UDP-161/162 (SMTP).

- Tick chọn **Log firewall traffic > Save**



- Kiểm tra: Trong mục tương tự

5.5. Yêu cầu rule khai báo Policy vừa đủ các địa chỉ nguồn, địa chỉ đích và port dịch vụ

- Với port quản trị:

- Mở chi tiết và cụ thể theo ip người dùng và hệ thống được cấp phép trên Firewall Office, Firewall WAN

- Mở theo dải không qua subnet 24 trên Firewall Server Farm, Firewall DMZ

- Với các port khác:
  - Mở không quá subnet 16
  - Mở không quá range 2000 port
- Với kết nối internet:
  - Được phép mở bất kỳ đích đến với kết nối đi internet

5.6. Yêu cầu rule khai báo phải chứa các thông tin phục vụ kiểm tra và rà soát ATTT

- Khi mở rule cần chú ý mở đúng theo: Title, zone, tags,...

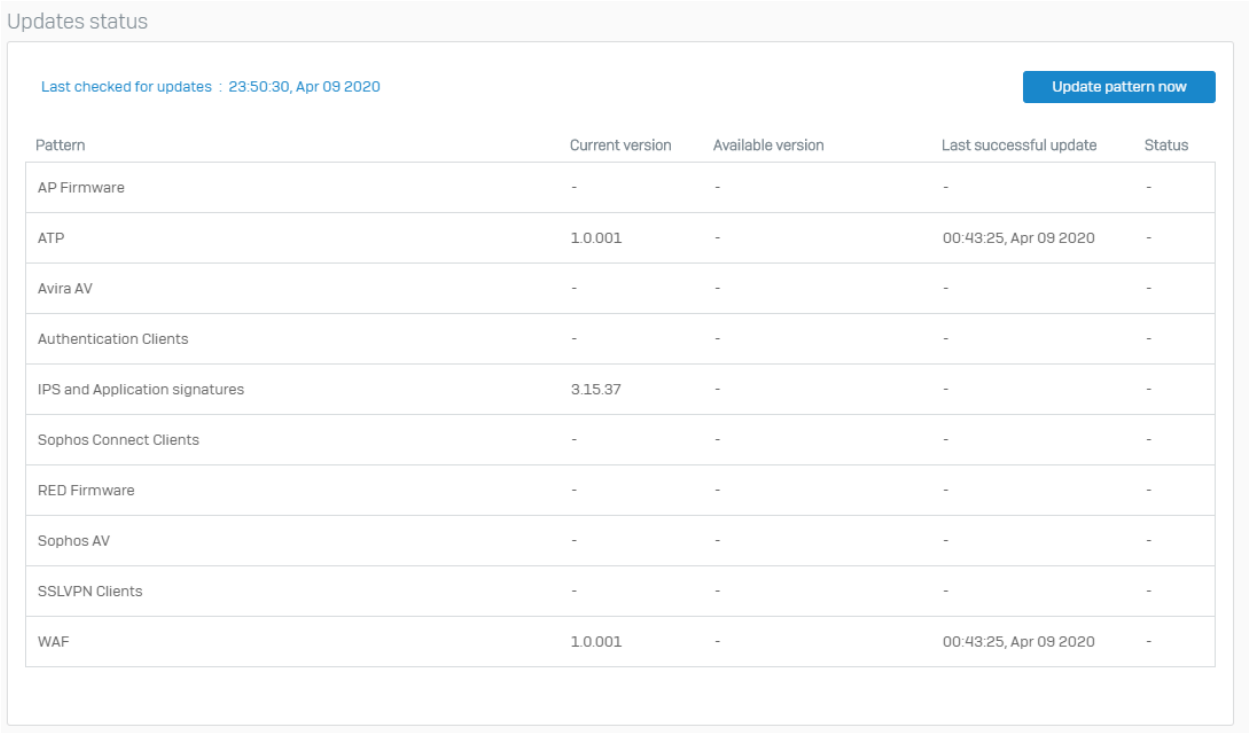
- Các rule quan trọng phải bật lưu logs hoặc bật lưu logs trên tất cả các rule đối với thiết bị nào đang đẩy về hệ thống phân tích logs tập trung

- Các rule cần phải có comment rõ ràng: ngày/tháng/năm mở rule - tên quản trị - rule mở cho mục đích gì - rule mở tạm thời thì cần có thời hạn cụ thể.

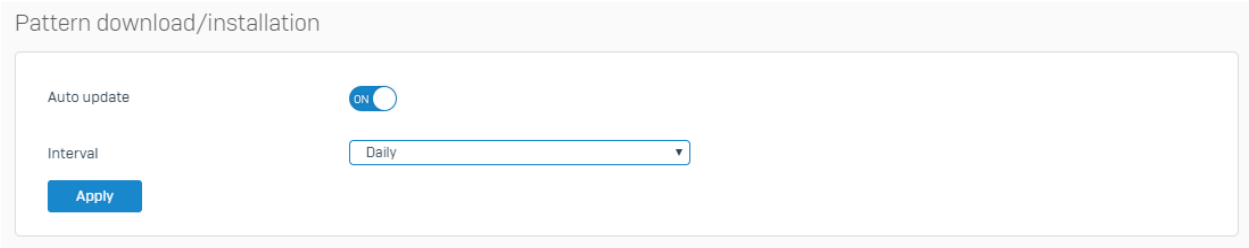
5.7. Yêu cầu IPS/IDS phải update bộ rule mới nhất và đầy đủ

- IPS/IDS phải update bộ rule mới nhất và đầy đủ được ban hành trên website và hệ thống cập nhật của hãng

  - Cấu hình
    - Chọn mục **System > Backup and Firmware > Pattern Updates**
    - Kiểm tra version IPS/IDS và so sánh với thông tin trên lasted version trên website hãng. Nếu chưa phải mới nhất click > **Update Pattern Now**



- Chọn mục **System > Backup and Firmware > Pattern Updates**

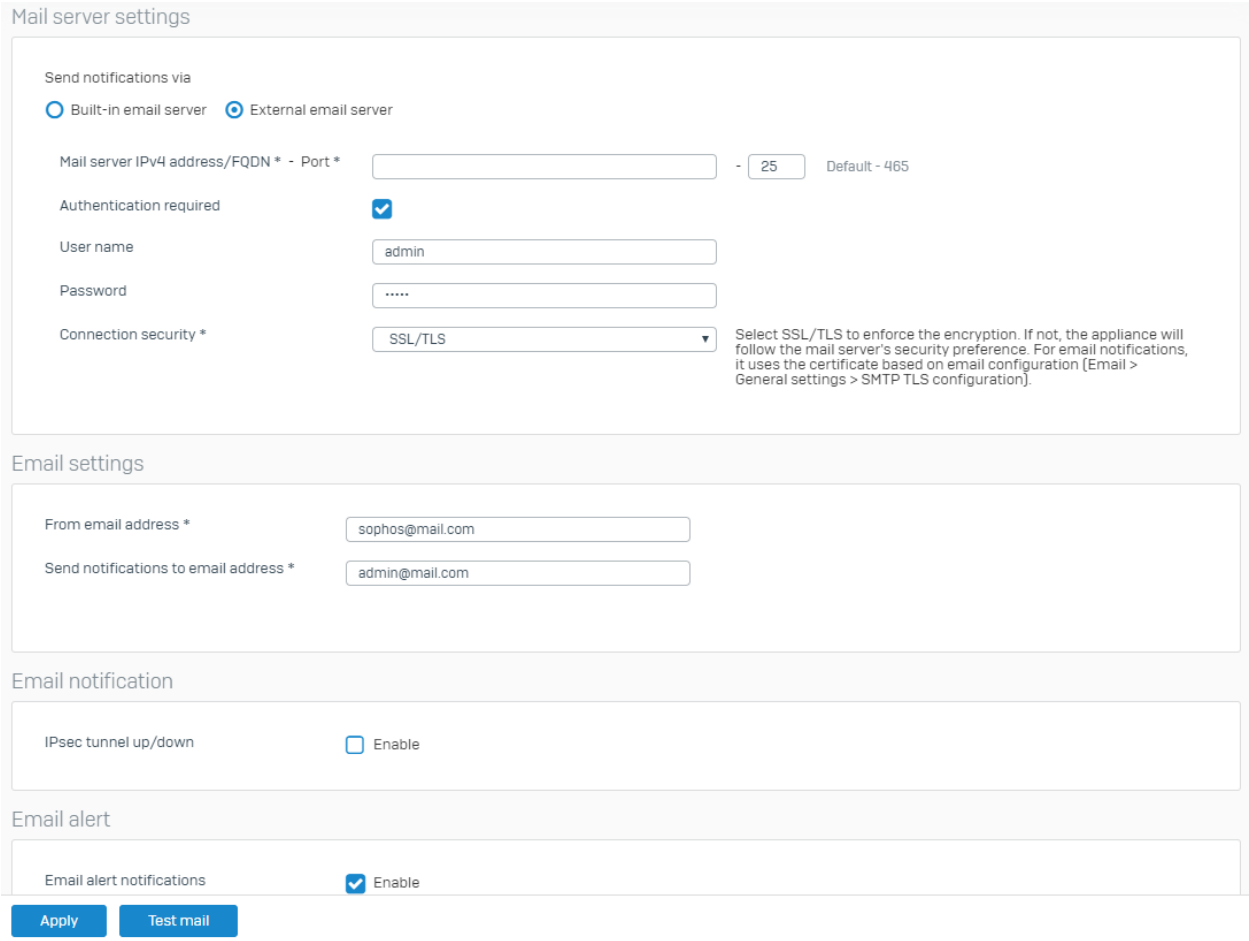


- Trong Pattern download/installation > **Auto update: Switch ON, Interval:** chọn **Daily > Apply**

5.8. Yêu cầu thiết lập gửi mail cảnh báo

- Thiết lập gửi mail cảnh báo về người quản trị khi có hành động phát hiện và chặn xâm nhập

- Cấu hình
  - Chọn mục **System > Administration > Notification**
  - Tick chọn **External email server** > Nhập các thông số cho email svr
  - Tick chọn **Email alert notification**
  - Nhập **from email address** và **to email address > Apply**



- Kiểm tra: trong mục tương tự.

IV. Hướng dẫn cho firewall FORTIGATE

1. Yêu cầu chung

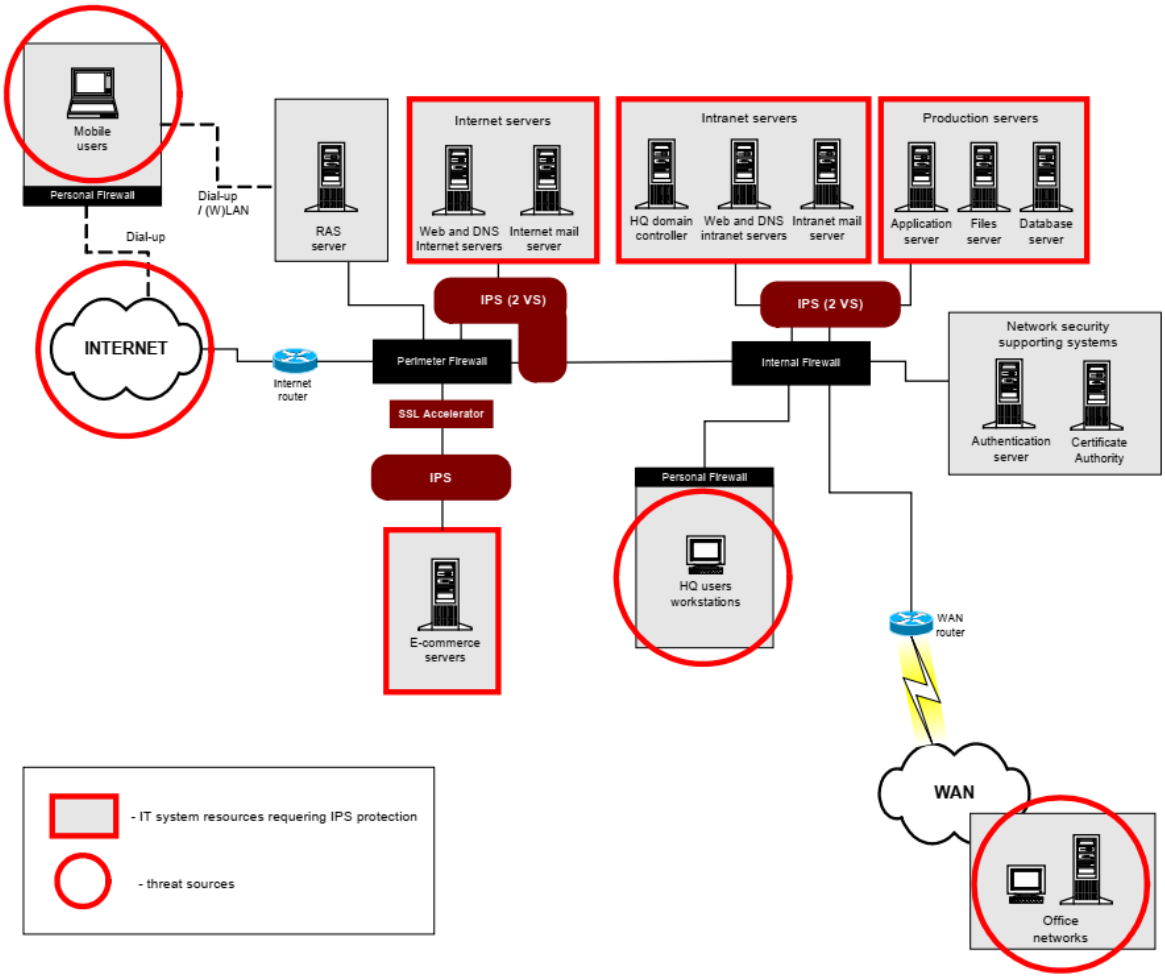
1.1. Yêu cầu phát hiện và chống tấn công từ internet

- Phải đặt IPS/IDS tại các vùng mạng mà monitor được tất cả các traffic in/out internet

  - Đặt tại vùng DMZ kết nối internet
  - Đặt tại vùng người dùng truy cập Internet.

- Phải đặt Firewall giữa kết nối từ Internet vào mạng nội bộ, đảm bảo toàn bộ traffic in/out internet phải đi qua Firewall

  - Đặt tại vùng DMZ kết nối internet
  - Đặt tại vùng người dùng truy cập Internet.



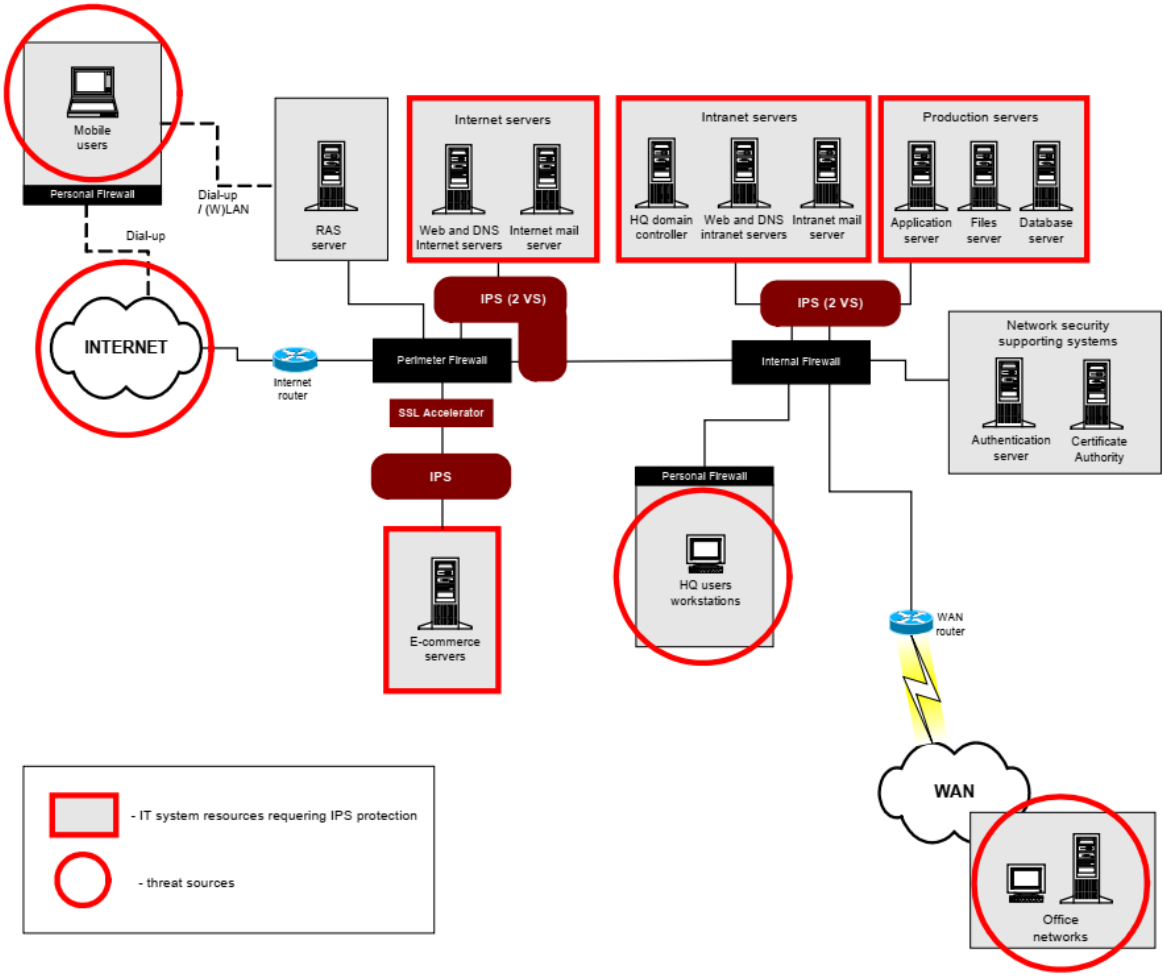
1.2. Yêu cầu phát hiện và chống tấn công từ nội bộ

- Phải đặt IPS/IDS tại các vùng mạng mà monitor được tất cả traffic in/out các hệ thống cần bảo vệ

- Đặt tại vùng Office kết nối vào mạng nội bộ.
- Đặt tại vùng WAN kết nối vào mạng nội bộ.
- Đặt tại vùng Server Farm kết nối vào mạng nội bộ.
- Đặt tại vùng Partner kết nối vào mạng nội bộ.

- Phải đặt Firewall giữa kết nối từ các hệ thống khác tới hệ thống cần bảo vệ, đảm bảo toàn bộ traffic in/out của vùng mạng cần bảo vệ đi qua Firewall

- Đặt tại vùng Office kết nối vào mạng nội bộ.
- Đặt tại vùng WAN kết nối vào mạng nội bộ.
- Đặt tại vùng Server Farm kết nối vào mạng nội bộ.
- Đặt tại vùng Partner kết nối vào mạng nội bộ.

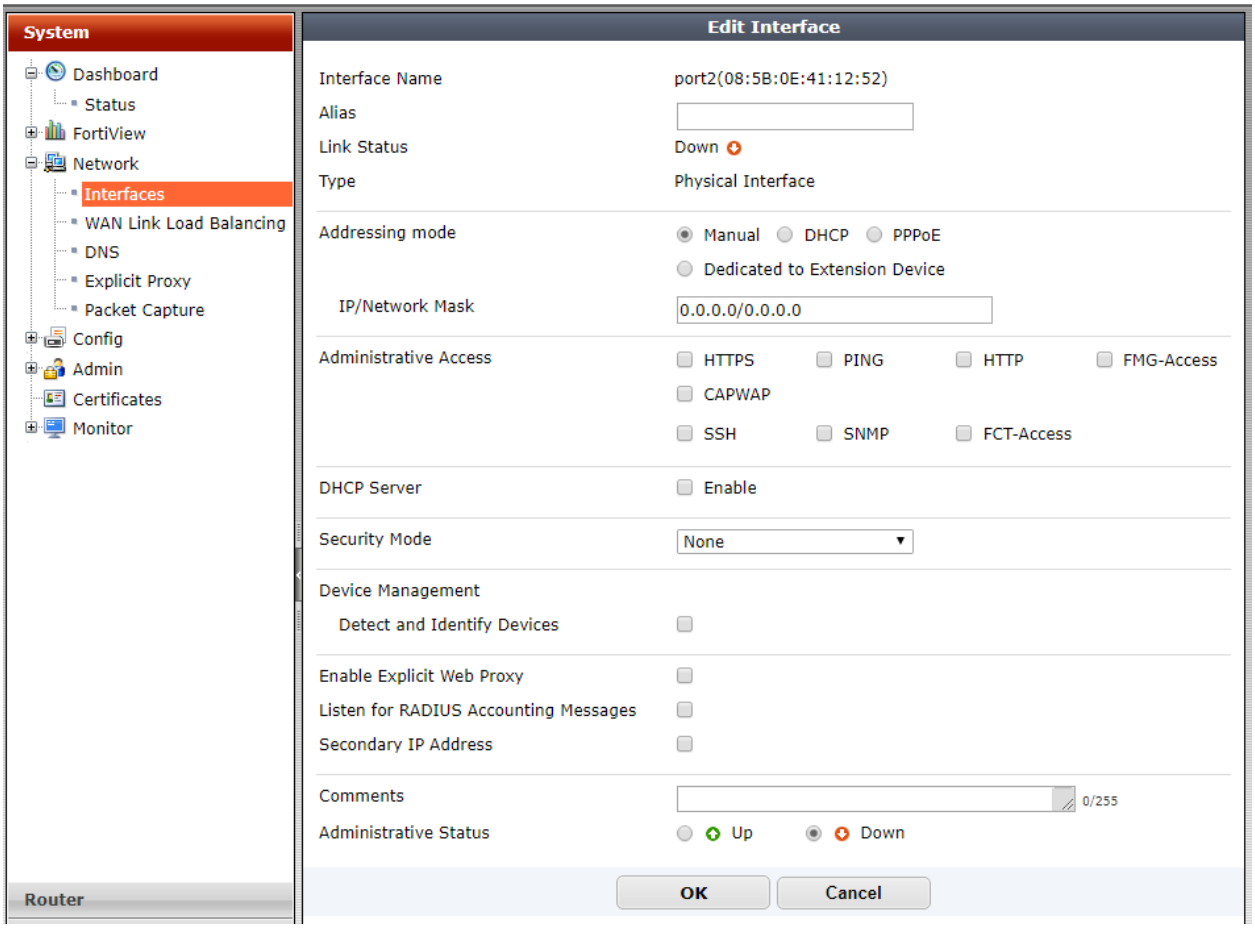


2. Cấu hình an ninh lớp 1

2.1. Yêu cầu shutdown port không sử dụng

- Shutdown tất cả các port không sử dụng trên thiết bị, chỉ bật lên khi có yêu cầu sử dụng

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Network > Interface**
    - Chọn Interface muốn shutdown

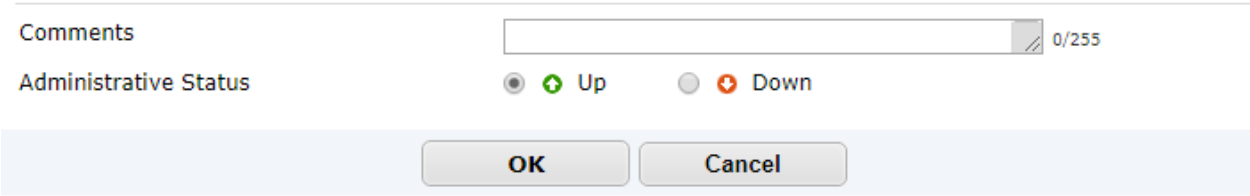


    - Tại **Administrative Status** chọn **Down**
    - Click **OK**
  - Kiểm tra: Trong mục tương tự

2.2. Yêu cầu mô tả kết nối rõ ràng

- Cổng đang bật phải có mô tả kết nối rõ ràng xác định được thông tin đấu nối của thiết bị đầu xa

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Network > Interface**
    - Chọn Interface muốn thêm mô tả
    - Nhập mô tả vào ô **Comment > OK** để apply cấu hình



- Kiểm tra: Trong mục tương tự

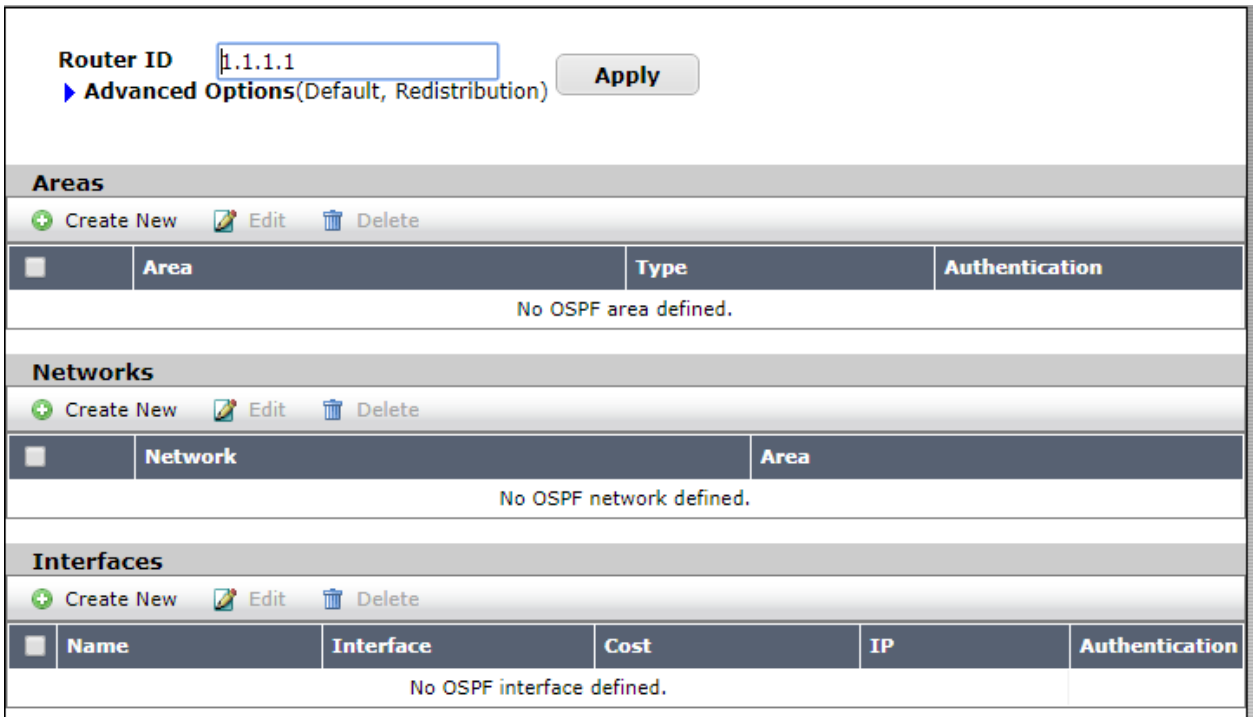
3. Cấu hình an ninh lớp 3

3.1. Xác thực cho các giao thức lớp 3

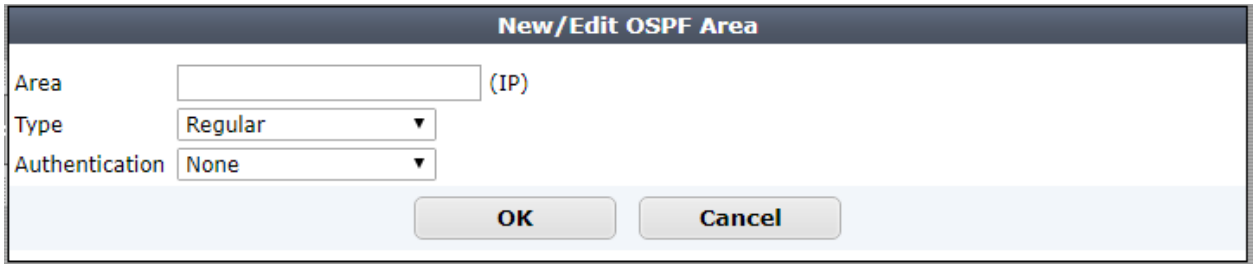
- VRRP, HSRP, GLBP, NSRP phải cấu hình xác thực cho giao thức giữa các thiết bị

Firewall Fortigate không hỗ trợ xác thực cho giao thức VRRP.

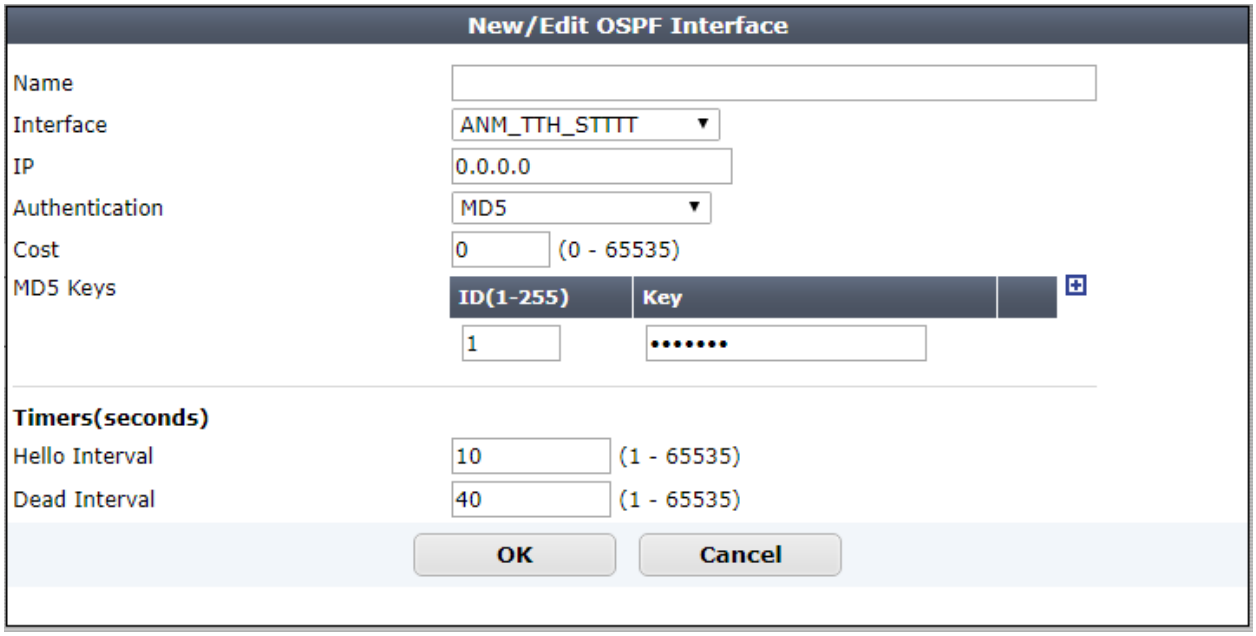
- OSPF phải thiết lập chuỗi xác thực có mã hóa giữa 2 thiết bị
  - Trên GUI:
    - Cấu hình:
      - Chọn mục **Router > OSPF**



      - Tại **Areas** chọn Area osfp cần cấu hình > Click **Edit**



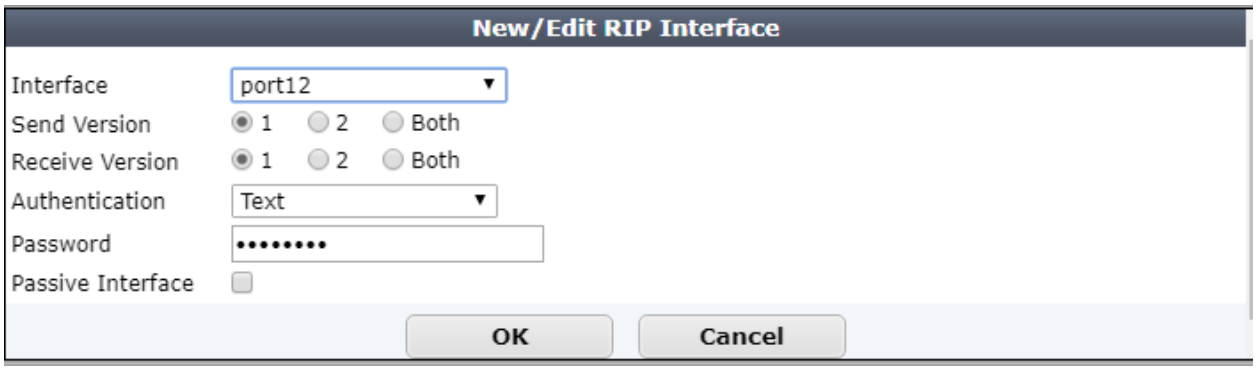
- **Authentication** > Tick chọn **MD5** > Click **OK**
- Tại **Interfaces** chọn interface cần cấu hình > Click **Edit**



- **Authentication** > Tick chọn **MD5**
- **MD5 Keys** > Điền chuỗi xác thực mong muốn > Click **OK**

  - Kiểm tra: Trong mục tương tự

- RIP phải thiết lập chuỗi xác thực có mã hóa giữa 2 thiết bị
  - Trên GUI:
    - Cấu hình:
      - Chọn mục **Router** > **RIP** > **Interfaces** > chọn Interface cần cấu hình > Click **Edit**



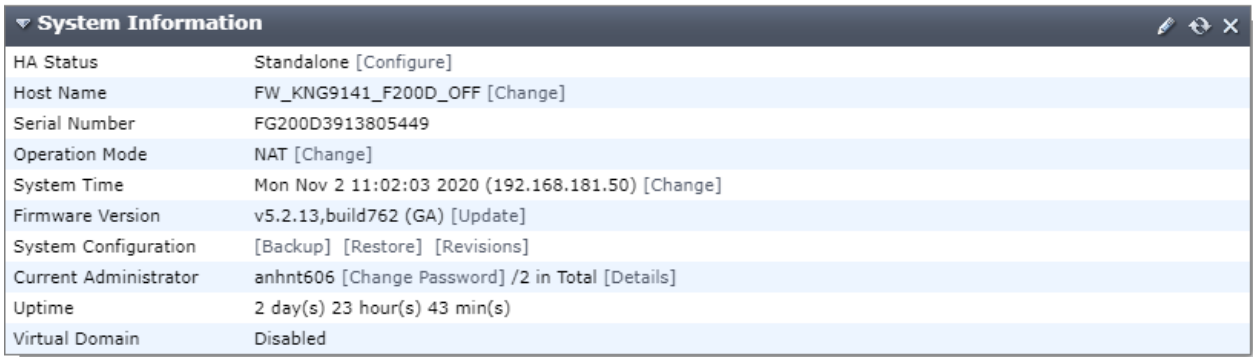
- **Athentication** chọn **Text** > điền đoạn chuỗi mong muốn vào ô **Password** > Click **OK**

4. Cấu hình quản trị

4.1. Yêu cầu về sao lưu cấu hình

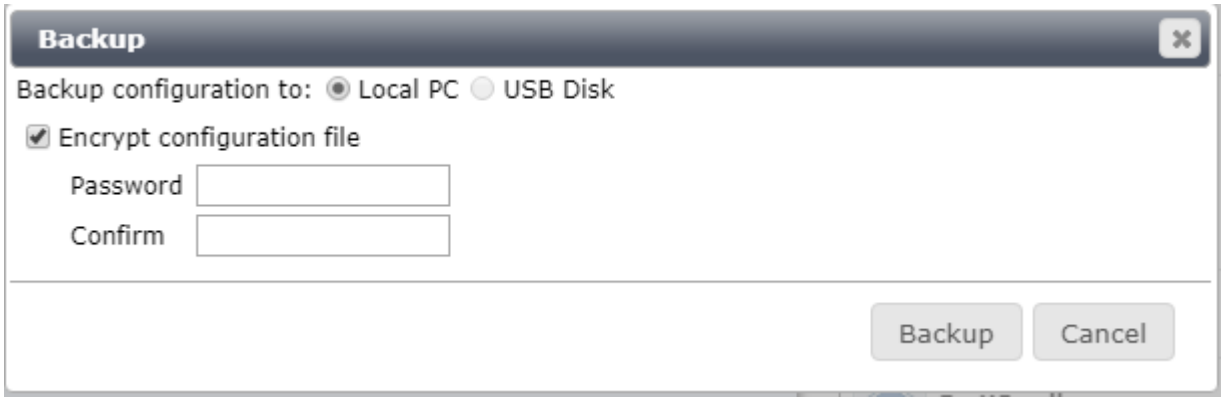
- Thiết bị phải được sử dụng phiên bản hệ điều hành và cập nhật các bản vá đảm bảo an toàn theo yêu cầu của bộ phận ATTT.

- Trên GUI:
  - Kiểm tra:
    - Chọn mục **System > Dashboard > Status**



- Lưu cấu hình trước khi tác động và định kì tối thiểu 01 lần/tuần. Lưu tối thiểu 02 bản gần nhất. Không lưu bản sao lưu trên máy tính cá nhân của quản trị viên.

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Dashboard > Status**
    - Trong **System Information** click chọn **Backup**



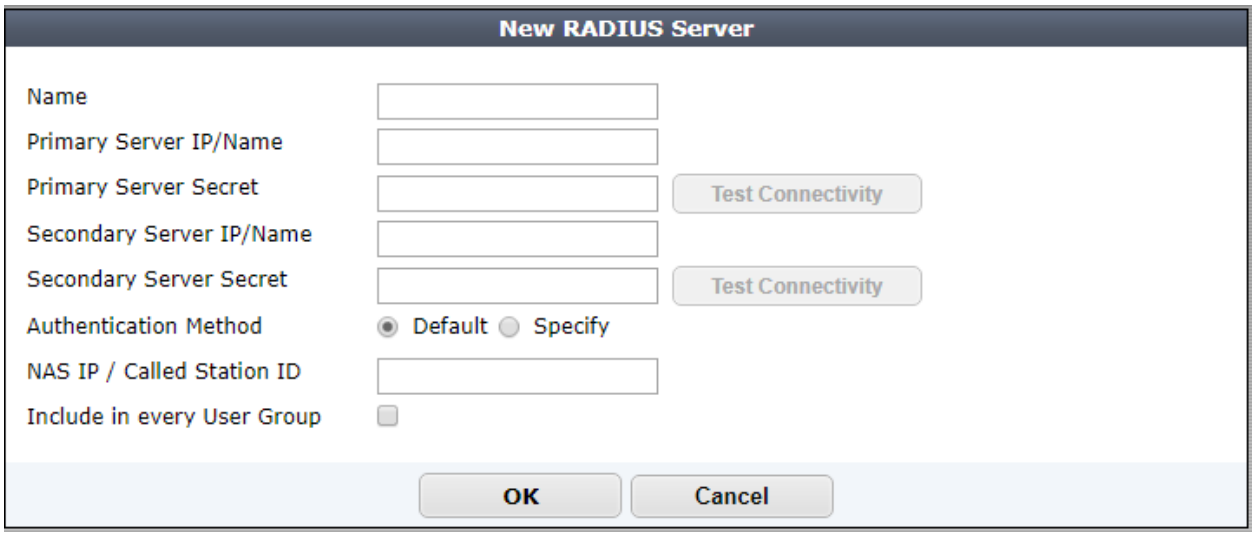
    - Tick chọn **Encrypt configuration file** > Điền Password > Click **Backup**
  - Kiểm tra: Kiểm tra file cấu hình được lưu trên máy tính đích.

4.2. Yêu cầu về quản lý tài khoản

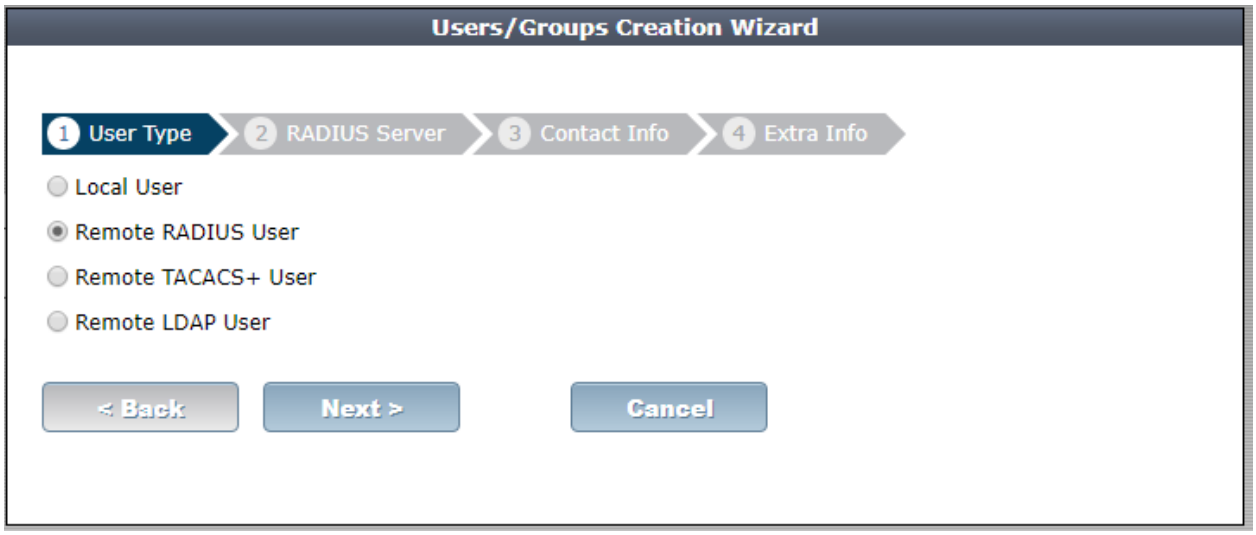
- Sử dụng hệ thống AAA để quản lý tài khoản người dùng tập trung (xác thực, phân quyền, ghi lịch sử tác động). Tối đa 02 tài khoản quản trị local dùng cho trường hợp khẩn cấp

- Trên GUI:

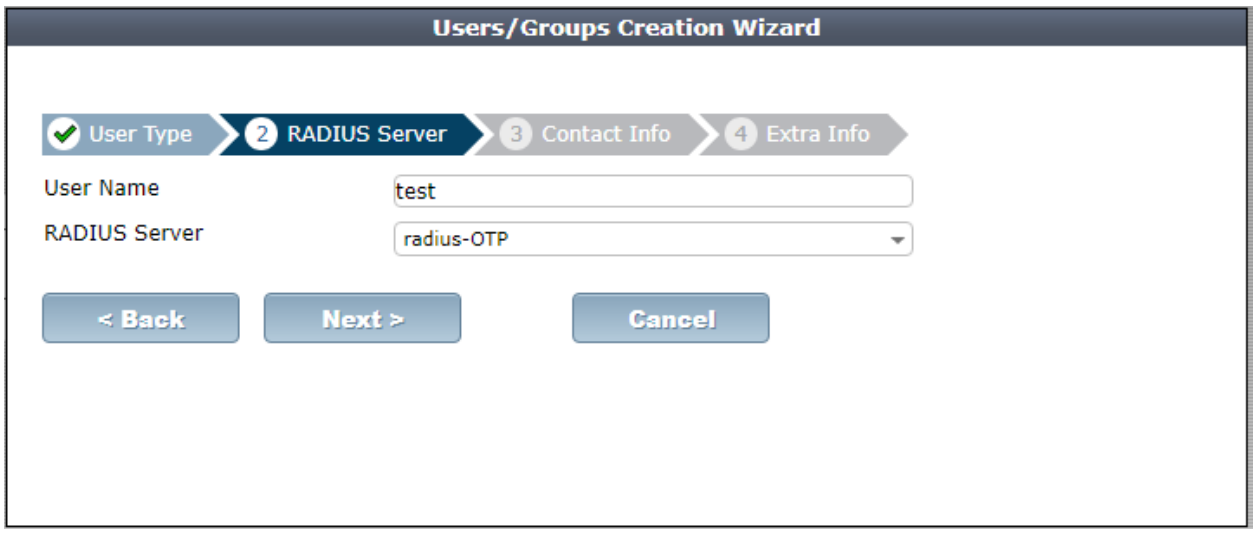
- Cấu hình:
  - Chọn mục User & **Device > Authentication** > Có thể chọn 1 trong các kiểu svr AAA tùy nhu cầu: **Radius, Tacacs+, LDAP, SSO...>** Click **Create New**



  - Nhập các thông số của AAA Server > **OK**
  - Chọn mục **User > User Definition** > Click **Create New**

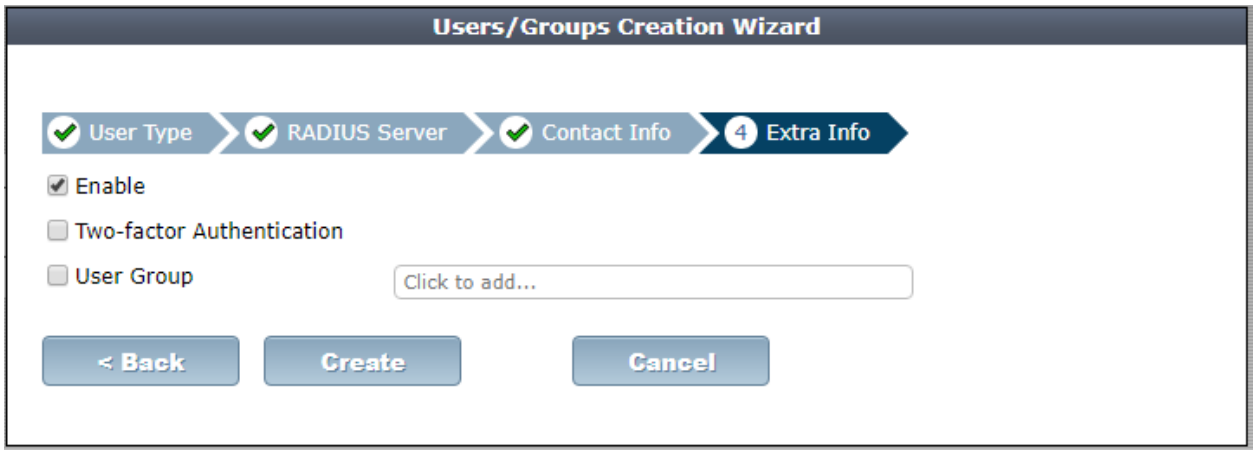


  - **User Type** chọn theo kiểu remote xác thực mong muốn > **Next**



- **Server**: Điền tên Username và chọn server vừa tạo ở trên > **Next**

- **Contact Info:** Điền thông tin email và SMS (có thể bỏ qua) > **Next**



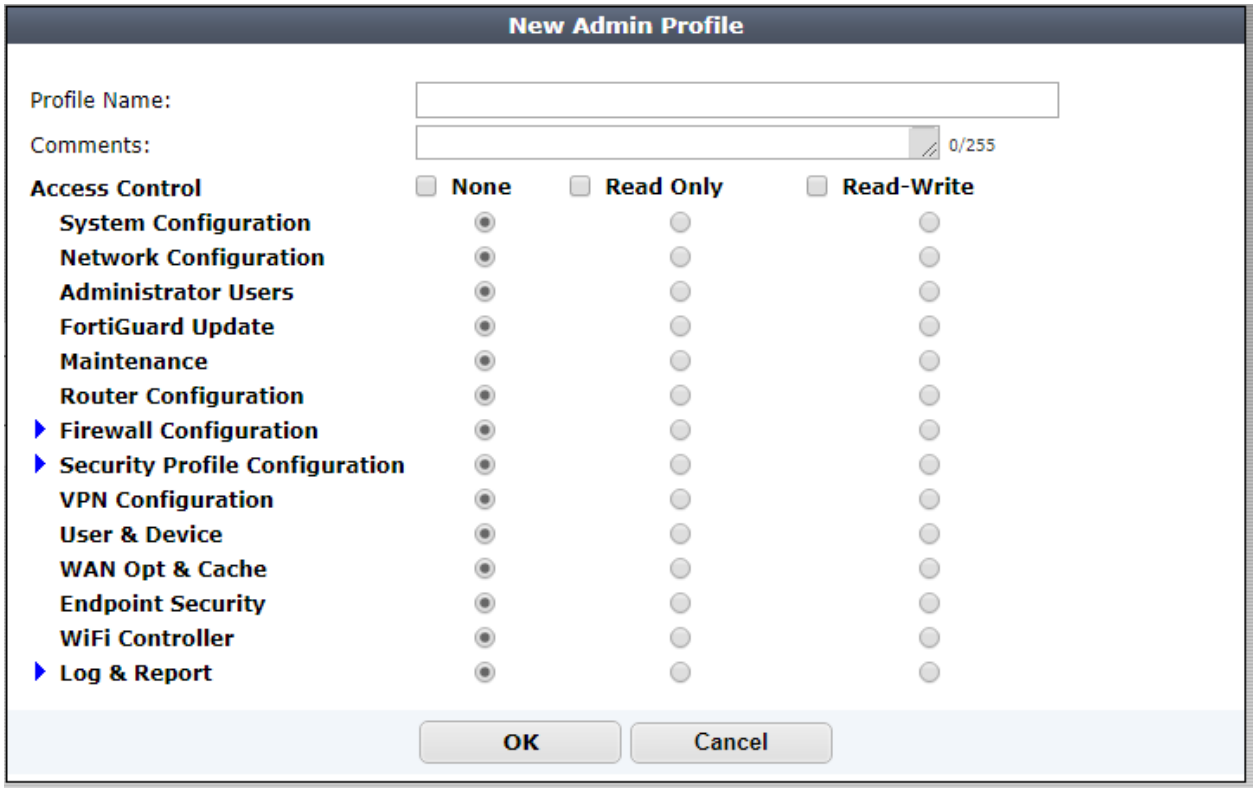
- **Extra Info:** Tick chọn **Enable** > Click **Create**

o Kiểm tra: Trong mục tương tự

- Quản trị viên phải sử dụng tài khoản được cấp riêng, phân quyền phù hợp trên local/AAA

<u>Đối với tài khoản Local</u>

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Admin > Admin Profile > Create New**
    - Chọn các quyền thích hợp cho **User** > Click **OK**



    - Chọn mục **System > Admin > Administrator** > Chọn User cần cấu hình > Click **Edit**

    - Tại **Administrator Profile**: Chọn profile vừa tạo ở trên > Click **OK**
  - Kiểm tra: Trong mục tương tự

<u>Đối với tài khoản AAA</u>

- Kiểm tra trực tiếp chính sách trên máy chủ AAA

- Đổi mật khẩu mặc định các tài khoản local của thiết bị

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Admin > Administrator >** Chọn account **admin** > **Edit > Change Password**
    - Đổi mật khẩu mặc định **> OK > OK** để apply cấu hình
  - Kiểm tra: Trong mục tương tự

- Thiết lập chính sách mật khẩu mạnh cho các tài khoản trên local/AAA. Khóa sau 5 lần đăng nhập sai, thời gian khóa tài khoản do đăng nhập sai là 10 phút

Đối với account local

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Admin > Settings**
    - Tick chọn **Enable Password Policy** > Điền các thông số phù hợp > **OK**

- Khóa sau 5 lần đăng nhập sai, thời gian khóa tài khoản do đăng nhập sai là 10 phút:

- Trên CLI:

```
config user setting
set auth-lockout-threshold 5
set auth-lockout-duration 300
end
```

  - Kiểm tra: Trong mục tương tự

Đối với account AAA

- Kiểm tra trực tiếp chính sách trên máy chủ AAA

4.3. Yêu cầu về kết nối quản trị

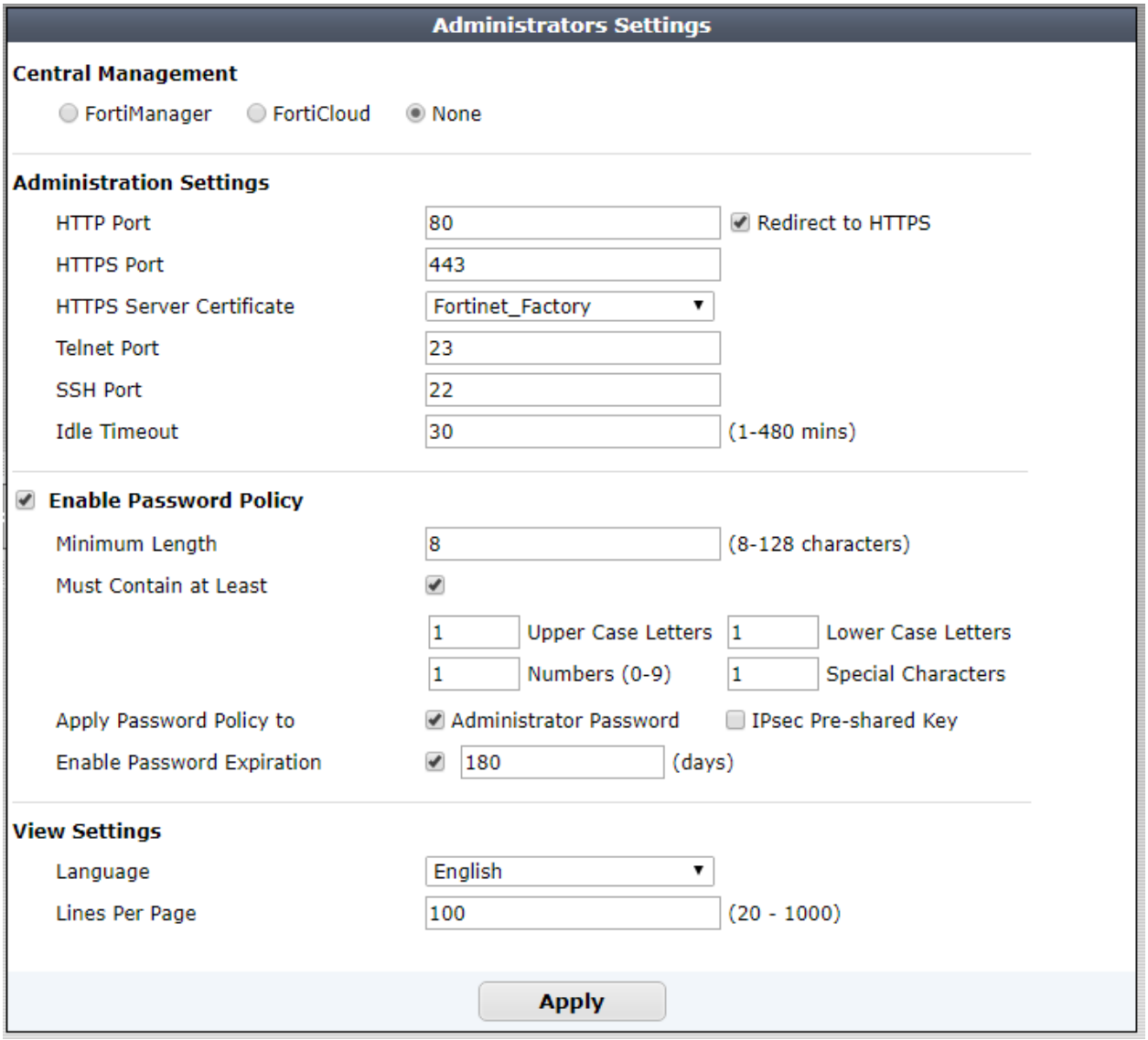
- Quản trị thiết bị qua VLAN quản trị dành riêng.
  - Kiểm tra trên cấu hình, đấu nối IP, quy hoạch VLAN quản trị

- Quản trị thiết bị qua kết nối trực tiếp Console hoặc kết nối từ xa an toàn, có mã hóa (SSHv2, HTTPS). Tắt các giao thức quản trị từ xa không an toàn (Telnet, HTTP)
  - Cấu hình:

- Trên CLI:

```
config system global
set admin-telnet disable
end
```

- Trên GUI:
  - Chọn mục **User & Device > Admin > Settings**
  - Tick chọn **Redirect to HTTPS**



- Giới hạn chỉ cho phép quản trị từ các IP theo danh sách đăng kí
  - Trên GUI:
    - Chọn mục **System > Admin > Administrator** > Chọn account **cần cấu hình** > **Edit** > Tick chọn **Restrict this Administrator Login from Trusted Hosts Only** > Điền IP quản trị > **OK**

- Kiểm tra: Trong mục tương tự

4.4. Yêu cầu cấu hình NTP

- Thiết bị phải được đồng bộ thời gian theo tối thiểu 01 máy chủ thời gian (NTP server)

- Trên CLI:
  - Cấu hình:

```
config system ntp
set type custom
set ntpsync enable
config ntpserver
edit 1
set server <ntp-server-ip>
next
edit 2
set server <other-ntp-server-ip>
end
```

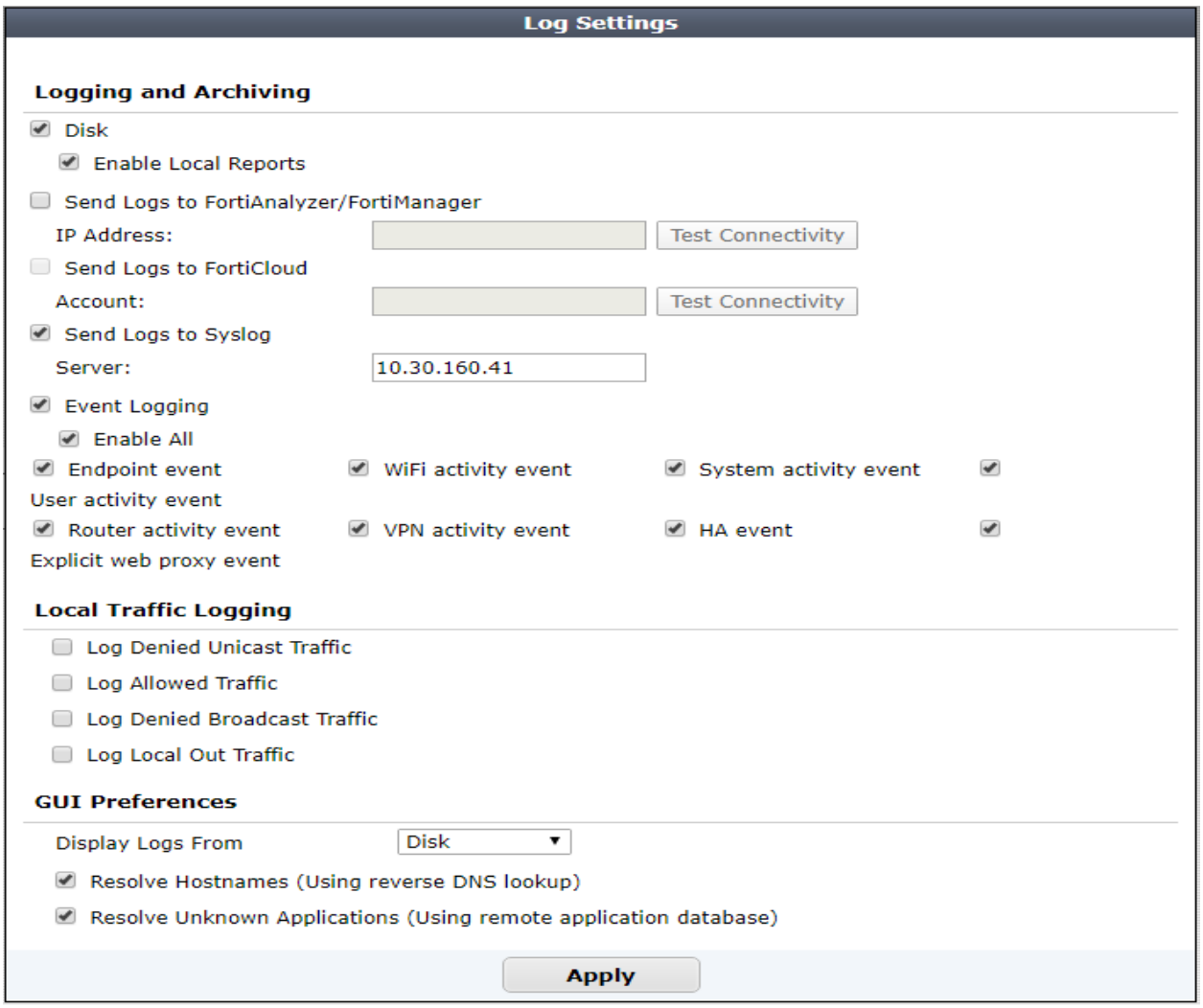
  - Kiểm tra:

```
get system ntp
```

4.5. Yêu cầu cấu hình log

- Thiết bị phải được thiết lập bật chế độ ghi log và cấu hình lưu log tập trung tối thiểu 06 tháng. Trong trường hợp không có hệ thống lưu log tập trung thực hiện thiết lập lưu trên local

- Trên GUI:
  - Cấu hình:
    - Chọn mục **Log & Report > Log Config > Log Settings**



- Tick chọn chế độ lưu log và các loại event cần lấy log > **Apply**

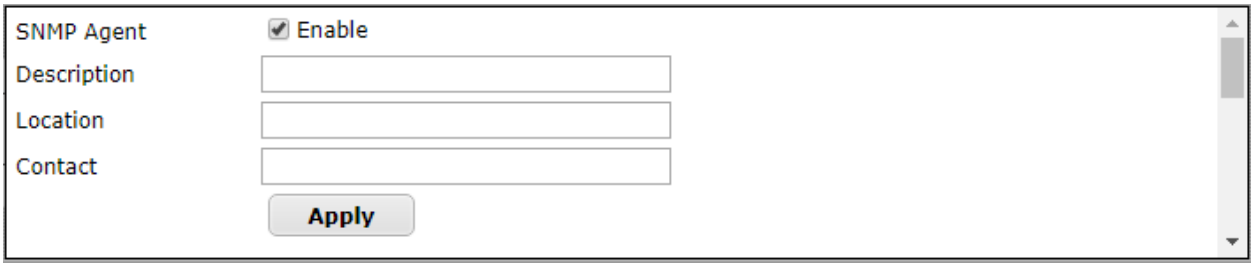
- Kiểm tra: Trong mục tương tự.

4.6. Yêu cầu cấu hình SNMP

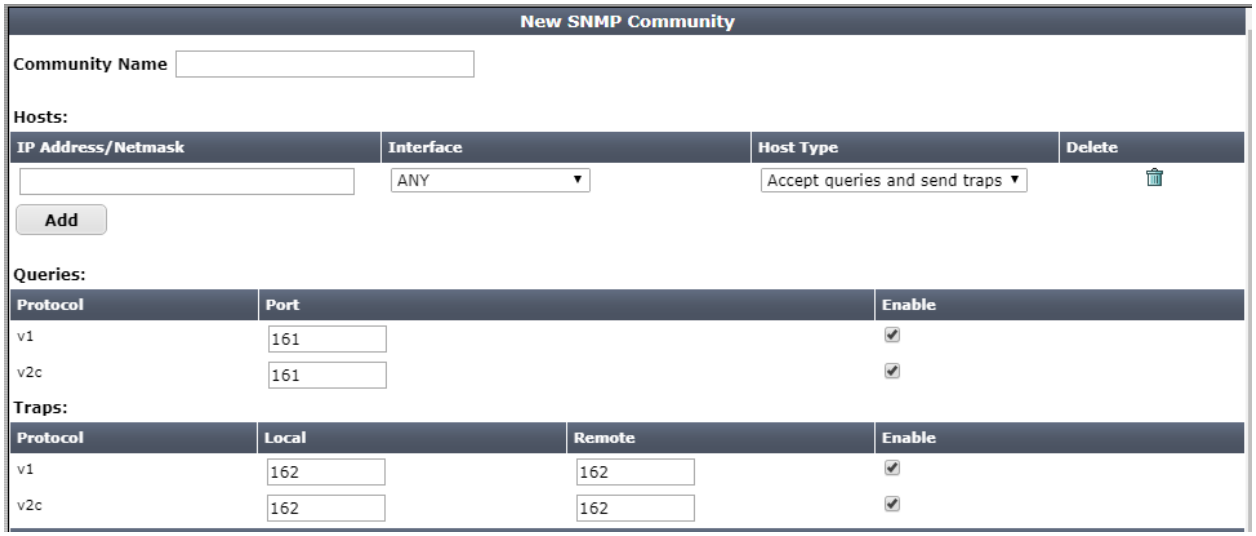
- SNMP phiên bản v2c, v3. SNMP theo chế độ read-only. Community string SNMP riêng. Xóa bỏ community string mặc định. Chỉ cho phép truy cập SNMP từ máy chủ giám sát.

<u>Với SNMP v2c</u>

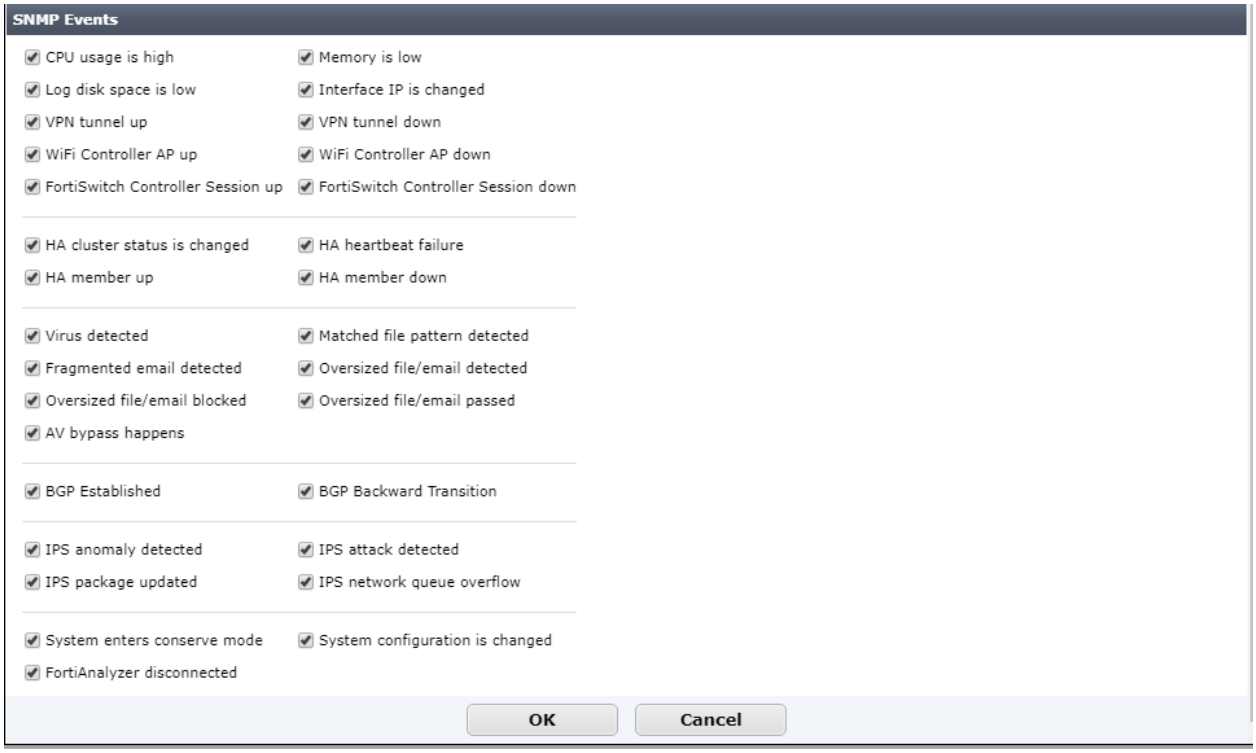
- Trên GUI:
  - Cấu hình:
    - Chọn mục **System** > **Config** > **SNMP** > Tick chọn **Enable SNMP Agent**



- Tại tab **SNMP v1/v2c > Create New**
- Điền chuỗi community vào ô **Community Name**
- Tại **Host**, Click **Add** > Điền IP của svr SNMP và Interface đấu nối của FW
- Tại Queries và Traps, Tick chọn **Enable** v2c



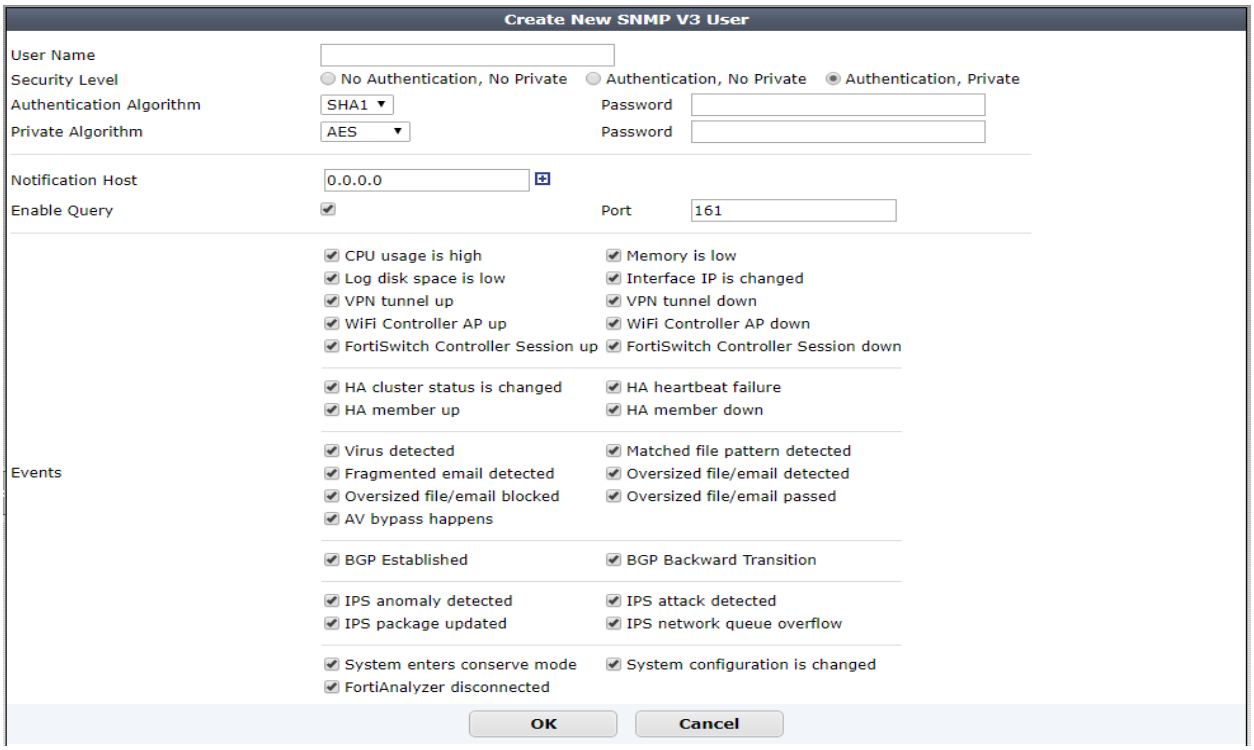
- Tại **SNMP Events**: Tick chọn các Event cần giám sát > **OK**



- Kiểm tra: trong mục tương tự

<u>Với SNMP v3</u>

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Config > SNMP** > Tick chọn **Enable SNMP Agent**
    - Tại tab **SNMP v3 > Create New**



    - Khai báo các thông tin cho SNMPv3 User
    - Tick chọn **Enable Query**
    - Tick chọn các Event cần giám sát > **OK**
  - Kiểm tra: trong mục tương tự

5. Thiết lập các tính năng an ninh

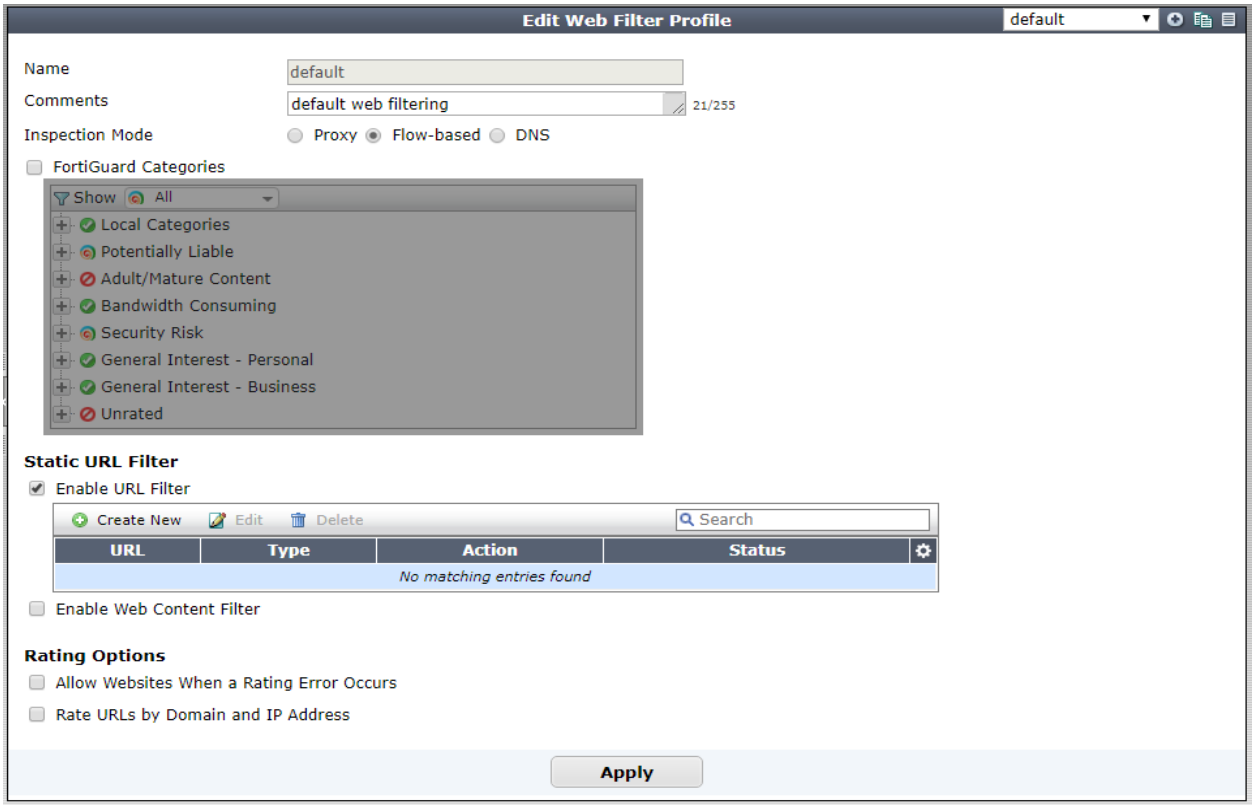
5.1. Yêu cầu bật tính năng phòng chống tấn công mạng trên các Firewall

- Bật và cấu hình các tính năng phòng chống tấn công mạng phù hợp với hệ thống CNTT được Firewall bảo vệ (IPS/IDS, UTM, Screening)

- Trên GUI:
  - Cấu hình:
    - Chọn mục **System > Config > Features** > Tick chọn các tính năng security mong muốn sử dụng **(cần có license)**

Đối với Web Filtering

- Cấu hình:
  - Tạo Web Filter Profile:
    - Chọn mục **Security Profiles > Web Filter**



    - Tick chọn **Enable Static URL Filter > Create New**

    - Điền thông tin URL, action mong muốn > Tick chọn **Enable** > **OK > Apply**

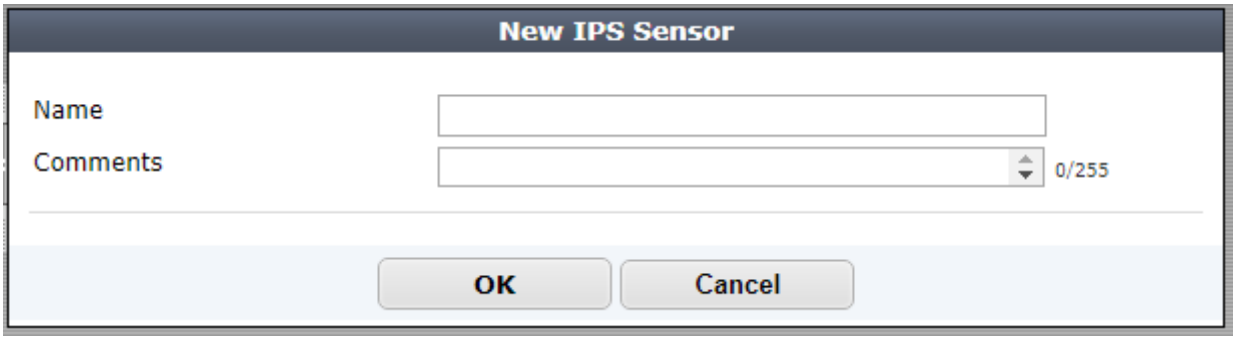
  - Gán Profile vào Firewall Policy
    - Chọn mục **Policies & Objects > Policy** > chọn policy cần URL-filtering (VD: Policy ra Internet...)

- Tại **Security Profiles**, Tick chọn **Web Filter** và chọn Profile vừa tạo > **OK**

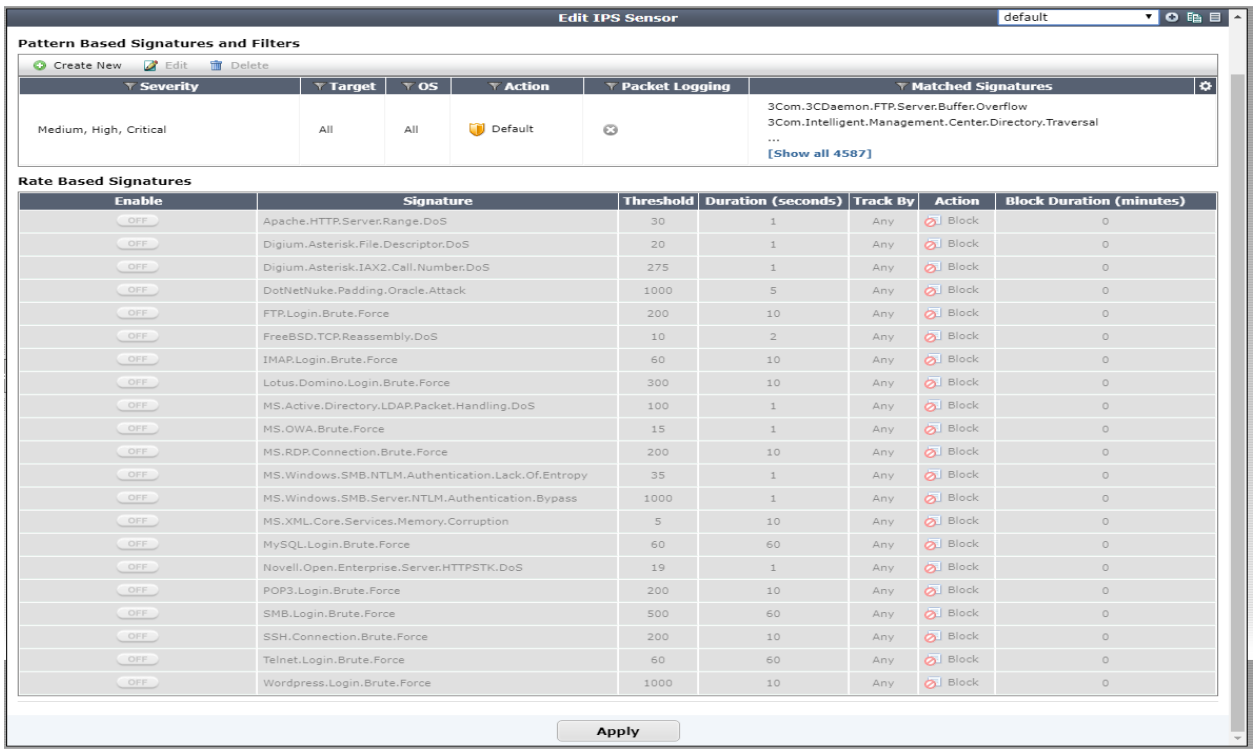
- Kiểm tra: Trong mục tương tự.

<u>Đối với Intrusion Protection</u>

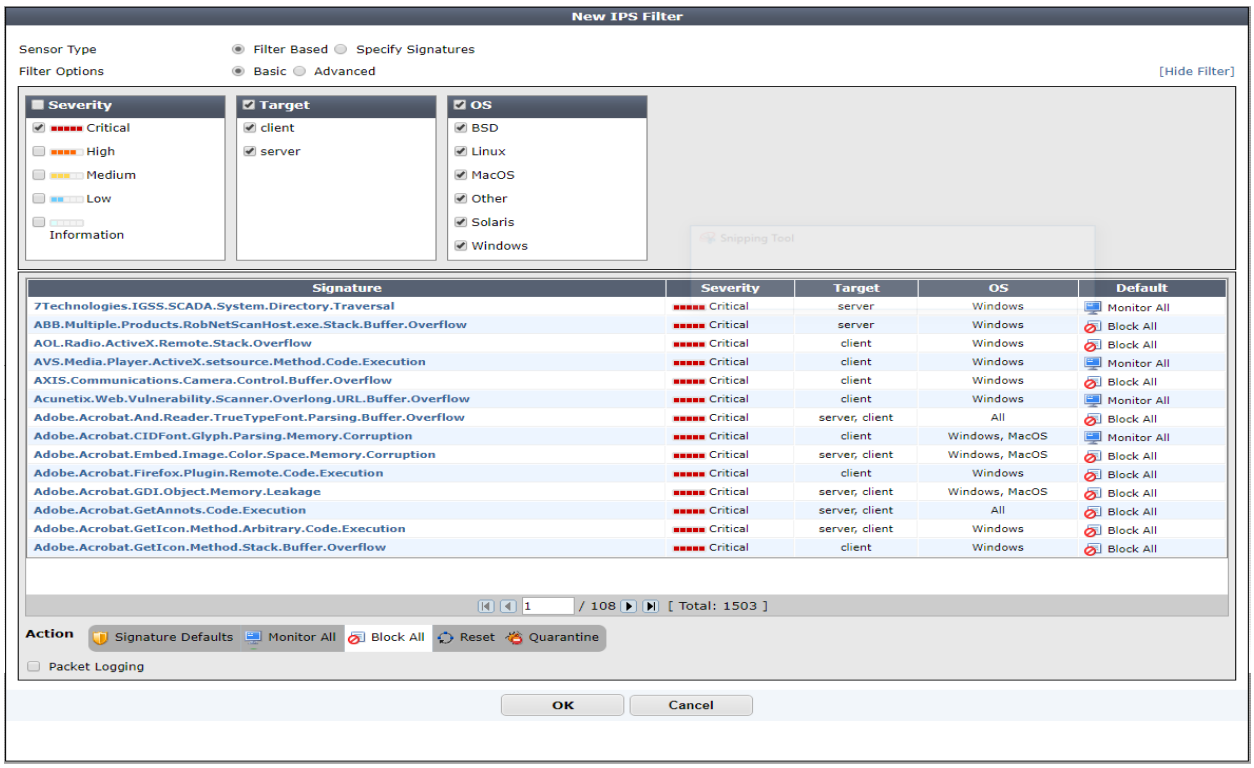
- Cấu hình:
  - Tạo IPS sensor
    - Chọn mục **Security Profiles > Intrusion Protection > Creat New**



    - Điền thông tin Name và Comments > **OK**
  - Add/Filter Signatures vào IPS sensor:
    - Chọn mục **Security Profiles > Intrusion Prevention** > chọn IPS sensor vừa tạo > **Edit**

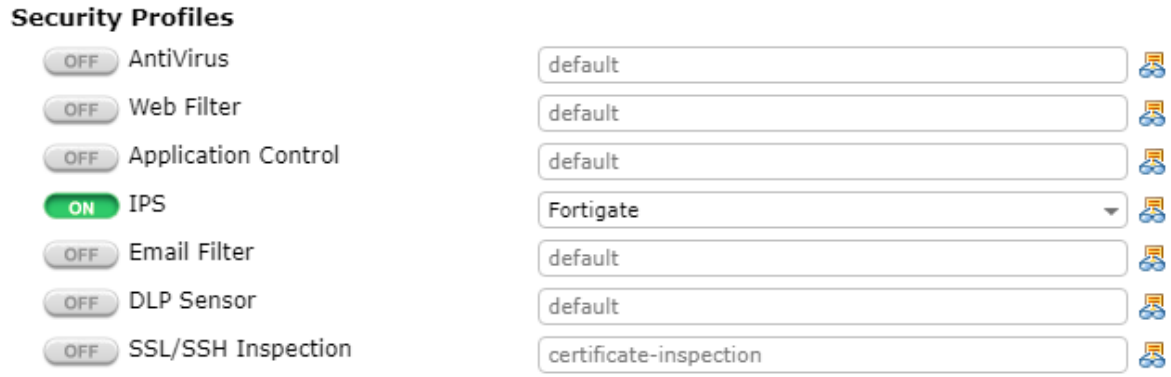


- Trong **Rate Based Signatures** (Signature về Ddos và Brute-Force): Tick chọn các signature mong muốn
- Trong **Pattern Based Signatures and Filters** chọn **Create New**



- Chọn các Signature mong muốn. Có thể chọn **Filter Based** (chọn hàng loạt theo severity, target, os, protocol, application) hoặc **Specify Signatures (**chọn từng signature riêng).
- Chọn **Action** mong muốn > Tick chọn **Packet Logging** (Optional) > **OK > Apply**

- Gán IPS sensor vào Firewall Policy
  - Chọn mục **Policies & Objects > Policy** > chọn policy cần URL-filtering (VD: Policy ra Internet...)
  - Tại **Security Profiles**, Tick chọn **IPS** và chọn Profile vừa tao > **OK**

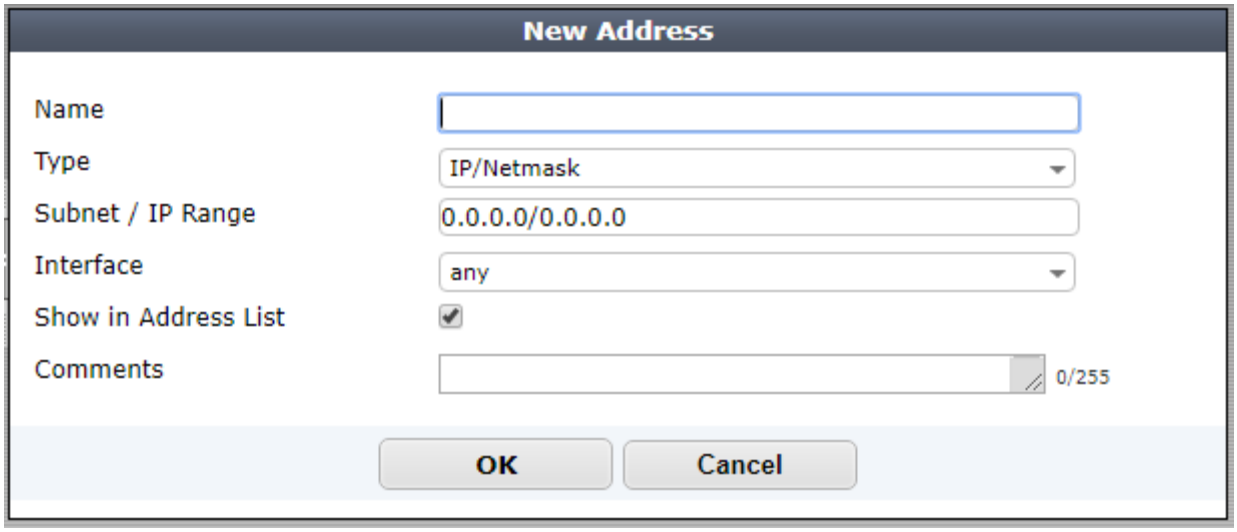


- Kiểm tra: Trong mục tương tự.

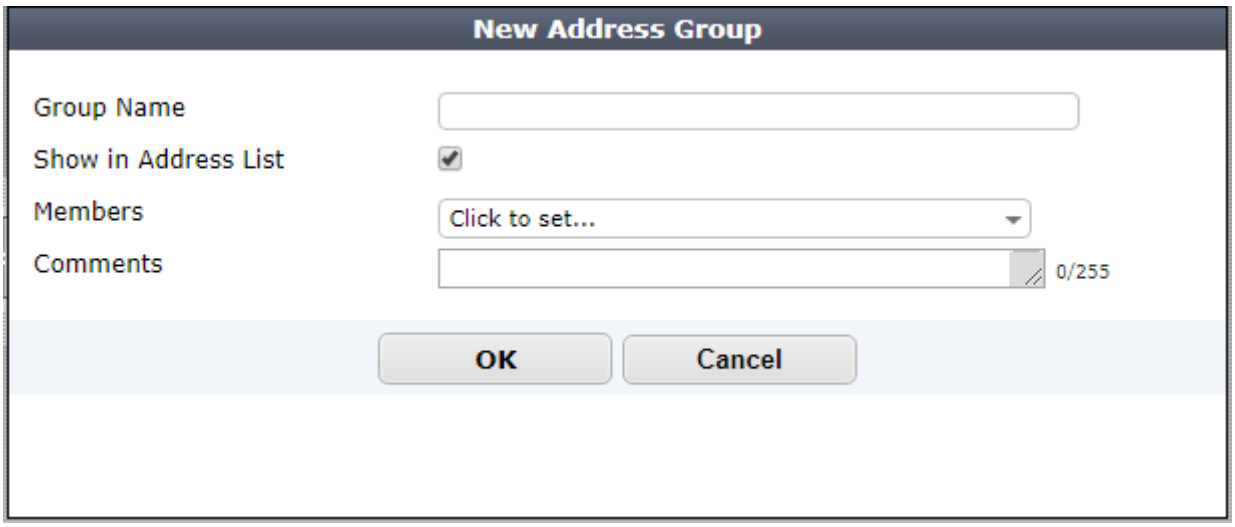
5.2. Yêu cầu rule phát hiện và ngăn chặn các kết nối C&C

- Khai báo phát hiện và ngăn chặn các kết nối C&C, các domain độc hại. Khai báo rule ở vị trí có hiệu lực đầu tiên

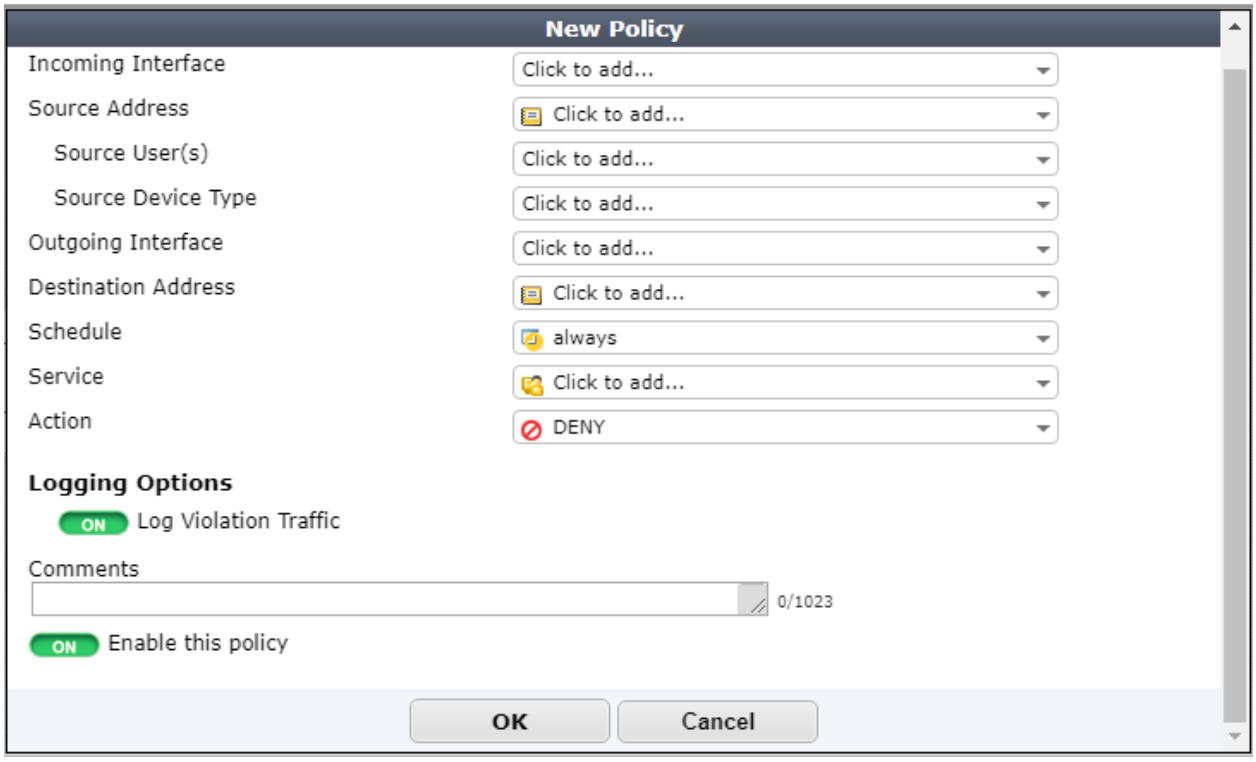
- Cấu hình
  - Chọn mục **Policies & Objects > Objects > Address > Create New**



  - Điền thông tin IP/Domain C&C cần chặn > **OK**
  - Chọn mục **Policies & Objects > Objects > Address > Create New Address Group.**



- Tại Member thêm các address đã tạo ở trên vào > **OK**
- Chọn mục **Policies & Objects > Policy > Ipv4 > Create New**



- **Incoming Interface:** chọn các Trust Zone, Interfaces. **Source Address** chọn **any**.
- **Outgoing Interface:** chọn các Untrust Zone, Interface. **Destination Address** chọn **Group C&C** vừa tạo.
- **Service** chọn **any**
- **Action:** chọn **Deny,** tick chọn **Log Violation traffic** và **Enable this policy > OK**
- **Kéo policy lên đầu tiên.**

o Kiểm tra: Trong mục tương tự

5.3. Yêu cầu rule phát hiện và chặn người dùng quản trị ra Internet

- Khai báo rule phát hiện và chặn người dùng quản trị ra Internet trực tiếp và qua Proxy, chỉ mở cho người dùng quản trị đến các hệ thống theo các port quản trị TCP-22 (SSH), (TCP-23 (Telnet), TCP-3389 (RDP),1433 (MS-SQL), TCP-1521->1527 (Oracle), TCP-3306 (Mysql), TCP-5432 (postgresql), TCP/UDP-161/162 (SMTP)

- Cấu hình
  - Tạo Address dải quản trị
    - Chọn mục **Policies & Objects > Objects > Address > Create New**
    - Điền dải IP quản trị > **OK**
  - Khai báo Policy
    - Chọn mục **Policies & Objects > Policy > Ipv4 > Create New**
    - **Incoming Interface:** chọn Zone, Interfaces có dải IP quản trị. **Source Address** chọn Address quản trị vừa tạo ở trên.
    - **Outgoing Interface:** chọn các Zone, Interface có kết nối ra Internet. **Destination Address** chọn **any**.
    - **Service** chọn **any**
    - **Action:** chọn **Deny,** tick chọn **Log Violation traffic** và **Enable this policy > OK**
  - Kiểm tra: Trong mục tương tự

5.4. Yêu cầu rule phát hiện và chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao

- Khai báo rule phát hiện và chặn kết nối port quản trị từ vùng có security level thấp sang vùng có security level cao:

- Internet: Level 1
- Wan: Level 2
- Office: Level 3
- DMZ: Level 4
- Server Farm: Level 5
- Cấu hình
  - Fortigate có rule mặc định chặn kết nối giữa các zone với nhau.

5.5. Yêu cầu rule khai báo Policy vừa đủ các địa chỉ nguồn, địa chỉ đích và port dịch vụ

- Với port quản trị:

- Mở chi tiết và cụ thể theo ip người dùng và hệ thống được cấp phép trên Firewall Office, Firewall WAN
- Mở theo dải không qua subnet 24 trên Firewall Server Farm, Firewall DMZ

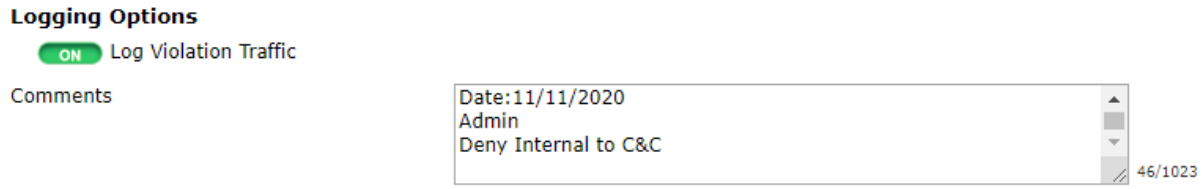
- Với các port khác:
  - Mở không quá subnet 16
  - Mở không quá range 2000 port
- Với kết nối internet:
  - Được phép mở bất kỳ đích đến với kết nối đi internet

5.6. Yêu cầu rule khai báo phải chứa các thông tin phục vụ kiểm tra và rà soát ATTT

- Khi mở rule cần chú ý mở đúng theo: Title, zone, tags,...

- Các rule quan trọng phải bật lưu logs hoặc bật lưu logs trên tất cả các rule đối với thiết bị nào đang đẩy về hệ thống phân tích logs tập trung

- Các rule cần phải có comment rõ ràng: ngày/tháng/năm mở rule - tên quản trị - rule mở cho mục đích gì - rule mở tạm thời thì cần có thời hạn cụ thể.



5.7. Yêu cầu IPS/IDS phải update bộ rule mới nhất và đầy đủ

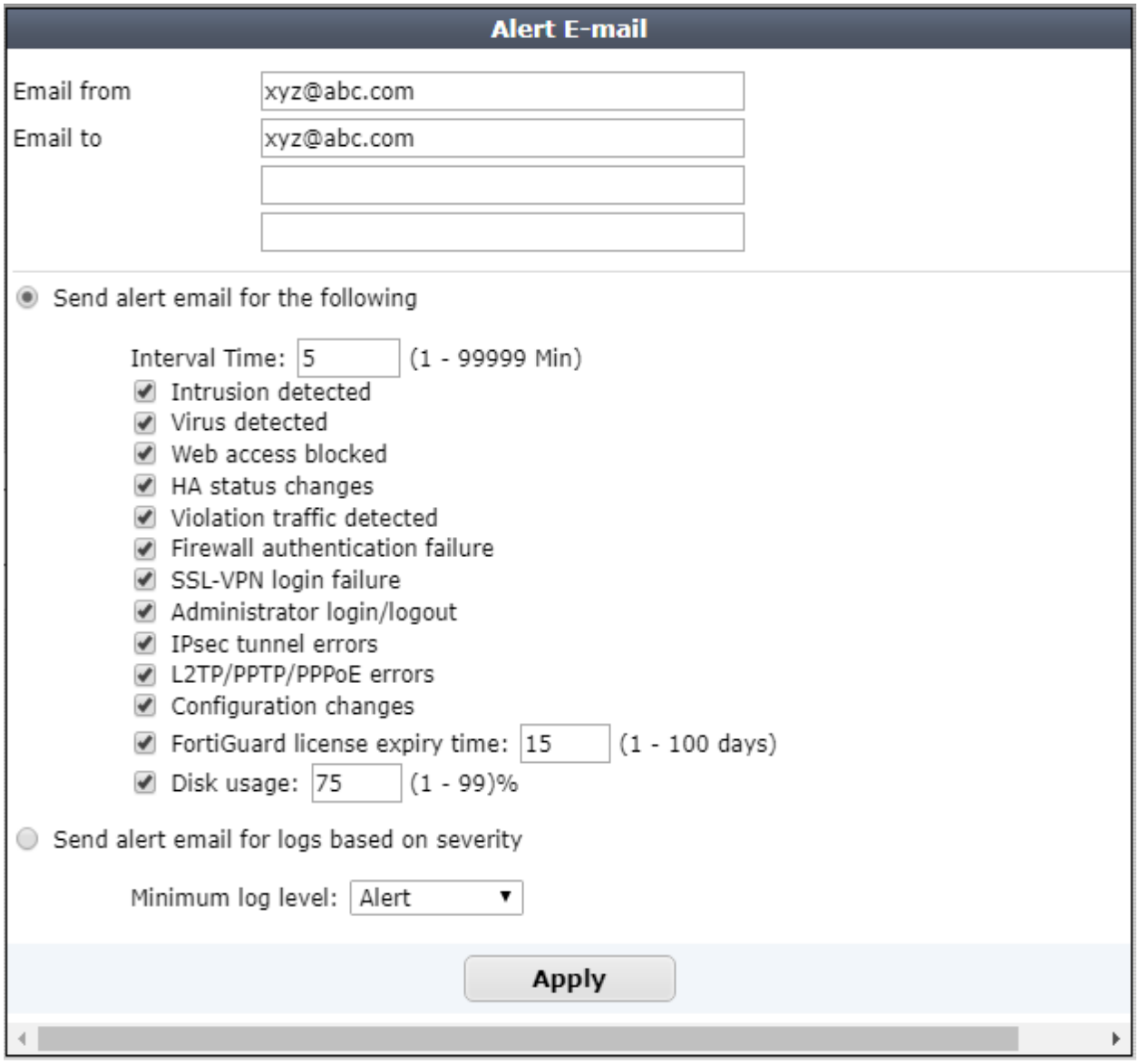
- IPS/IDS phải update bộ rule mới nhất và đầy đủ được ban hành trên website và hệ thống cập nhật của hãng

5.8. Yêu cầu thiết lập gửi mail cảnh báo

- Thiết lập gửi mail cảnh báo về người quản trị khi có hành động phát hiện và chặn xâm nhập.

- Trên GUI:
  - Cấu hình
    - Chọn mục **System > Config > Advanced > Email Service**
    - Điền các thông tin về Email server > **Apply**

- Chọn mục **Log & Report > Log Config > Alert Email**
- Điền thông tin Email nhận cảnh báo
- Tick chọn các loại event và level log gửi email > **Apply**



- Kiểm tra: Trong mục tương tự

Phụ lục 15.
HƯỚNG DẪN THIẾT LẬP CẤU HÌNH ATTT CHO THIẾT BỊ THIẾT BỊ MẠNG CISCO VÀ JUNIPER

1. Cấu hình chung

1.1. Đưa các thiết bị về trạng thái cấu hình mặc định trước khi triển khai tích hợp vào mạng lưới

+ ***Với Cisco IOS:***

 # write erase

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

<Press Enter key>

 # reload

Proceed with reload? [confirm]

<Press Enter key>

+ ***Với Cisco NX-OS:***

 # write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y

+ ***Với Juniper Junos 11.1 trở lên:***

EX> request system zeroize

+ ***Với Juniper Junos 11.1 trở xuống:***

EX> request system configuration rescue delete

EX> start shell user root

Password:

root@EX% cd /config

*root@EX% rm -rf juniper.conf**

root@EX% cd /config/db/config

*root@EX% rm -rf juniper.conf.**

root@EX% reboot

1.2. Đảm bảo sử dụng firmware, phần mềm và bản vá không tồn tại lỗi ATTT

- Đảm bảo sử dụng firmware, phần mềm và bản vá không có lỗ hổng ATTT trong CVE đã được công bố

+ Kiểm tra version, firmware đang sử dụng của thiết bị:

+ ***Với Cisco IOS:***

 # show version

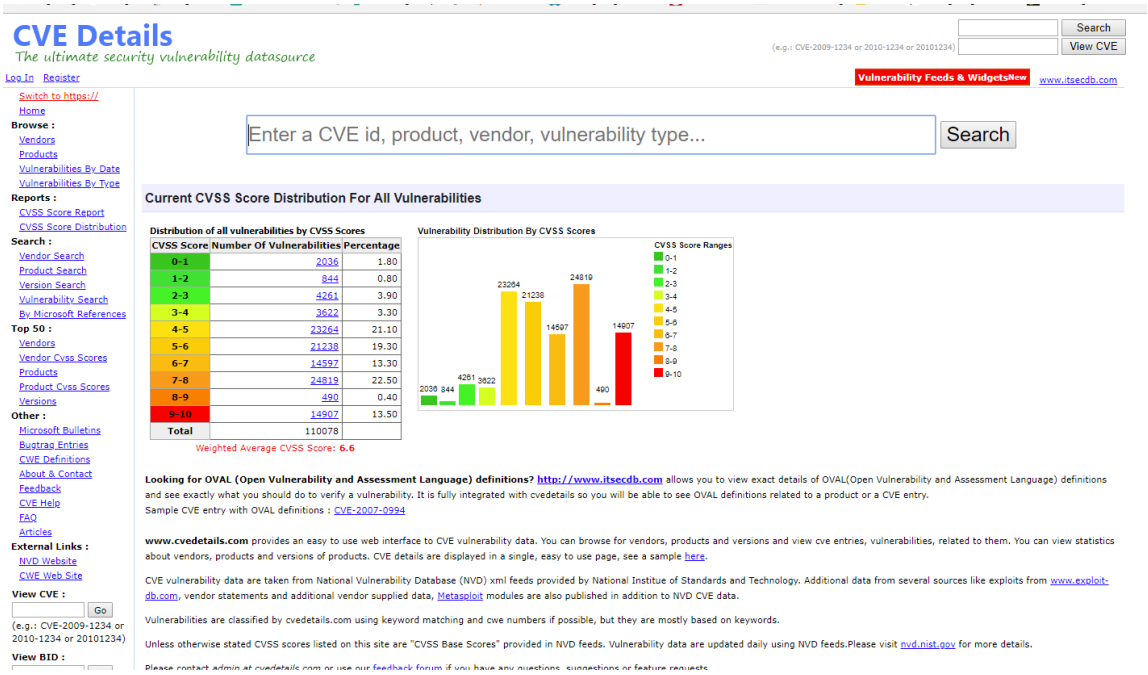
+ ***Với Cisco NX-OS:***

 # show version

+ ***Với Juniper Junos:***

EX> show version

+ Kiểm tra CVE của thiết bị có tồn tại hay không bằng cách truy cập vào trang https://www.cvedetails.com/ nhập tên version và thiết bị vào để check



2. Cấu hình an ninh lớp 1

2.1. Yêu cầu phải shutdown port không sử dụng

- Shutdown tất cả các port không sử dụng trên thiết bị, chỉ bật lên khi có yêu cầu sử dụng

+ Lệnh cấu hình:

+ ***Với Cisco IOS:***

(config)# interface <interface-name>

(config-if)# shutdown

+ ***Với Cisco NX-OS:***

(config)# interface <interface-name>

(config-if)# shutdown

+ ***Với Juniper Junos:***

<hostname> set interfaces <interface-name> disable

+ Lệnh kiểm tra:

+ ***Với Cisco IOS:***

 # show interfaces <interface-name>

 # show ip interface brief

+ ***Với Cisco NX-OS:***

 # show interfaces <interface-name>

 # show ip interface brief

+ ***Với Juniper Junos:***

<hostname> show interfaces <interface-name> | match Phy

2.2. Yêu cầu mô tả kết nối rõ ràng

- Cổng đang bật phải có mô tả kết nối rõ ràng xác định được thông tin đấu nối của thiết bị đầu xa

+ Lệnh cấu hình:

+ ***Với Cisco IOS:***

(config)# interface <interface-name>

(config-if)# description <if-description>

+ ***Với Cisco NX-OS:***

(config)# interface <interface-name>

(config-if)# description <if-description>

+ ***Với Juniper Junos:***

<hostname> set interfaces <interface-name> description <if-description>

+ Lệnh kiểm tra:

+ ***Với Cisco IOS:***

 # show interfaces description

+ ***Với Cisco NX-OS:***

 # show interfaces description

+ ***Với Juniper Junos:***

<hostname> show interfaces descriptions | match <interface_name>

3. Cấu hình an ninh lớp 2

3.1. Yêu cầu không sử dụng vlan default

- Bỏ cấu hình vlan default (thường là vlan 1) trên các interface

+ Lệnh cấu hình:

+ ***Với Cisco IOS:***

(config)# interface <interface-name>

(config-if)# switchport mode access

(config-if)# switchport access vlan <vlan-id khác>

+ ***Với Cisco NX-OS:***

(config)# interface <interface-name>

(config-if)# switchport mode access

(config-if)# switchport access vlan <vlan-id khác>

+ ***Với Juniper Junos:***

<hostname> set interface <interface-name> unit 0 family ethernet-switching port-mode access

<hostname> set interface <interface-name> unit 0 family ethernet-switching vlan members <vlan-id khác>

+ Lệnh kiểm tra:

+ ***Với Cisco IOS:***

 # show vlan

+ ***Với Cisco NX-OS:***

 # show vlan

+ ***Với Juniper Junos:***

<hostname> show vlans

3.2. Yêu cầu cấu hình chính xác các cổng trunk, cổng access theo đúng thiết kế

- Cấu hình chính xác các cổng trunk, cổng access theo đúng thiết kế đã phê duyệt.

+ Lệnh cấu hình:

+ ***Với Cisco IOS:***

//Doi voi cac port access

(config)# interface <access-port>

(config-if)#switchport mode access

//Doi voi cac port trunk

(config)# interface <trunk-port>

(config-if)#switchport mode trunk

+ ***Với Cisco NX-OS:***

//Doi voi cac port access

(config)# interface <access-port>

(config-if)#switchport mode access

//Doi voi cac port trunk

(config)# interface <trunk-port>

(config-if)#switchport mode trunk

+ ***Với Juniper Junos:***

//Doi voi cac port access

<hostname> set interface <interface-name> unit 0 family ethernet-switching port-mode access

//Doi voi cac port trunk

<hostname> set interface <interface-name> unit 0 family ethernet-switching port-mode trunk

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show interfaces <interface-name> switchport

 # show running-config

 # show interfaces trunk

+***Với Cisco NX-OS:***

 # show interfaces <interface-name> switchport

 # show running-config

 # show interfaces trunk

+***Với Juniper Junos:***

<hostname> show vlans

<hostname> show ethernet-switching interfaces

- Đối với cổng trunk phải giới hạn những vlan được phép đi cổng trunk, không cho phép vlan default đi qua

+ Lệnh cấu hình:

+***Với Cisco IOS:***

(config)# interface <trunk-port>

(config-if)# switchport trunk allowed vlan except 1

(config-if)# switchport trunk allowed vlan <vlan-list> (ex: 5-10,11,13-19)

Lưu ý: *Các giá trị vlan được trunk sẽ ghi đè lên vlan-list được trunk trước đó. Nếu muốn trunk thêm một số vlan và giữ nguyên các vlan trunking trước đó thì dùng câu lệnh:*

(config-if)# switchport trunk allowed vlan add <vlan-list>

+***Với Cisco NX-OS:***

(config)# interface <trunk-port>

(config-if)# switchport trunk allowed vlan except 1

(config-if)# switchport trunk allowed vlan <vlan-list> (ex: 5-10,11,13-19)

***Lưu ý**: Các giá trị vlan được trunk sẽ ghi đè lên vlan-list được trunk trước đó. Nếu muốn trunk thêm một số vlan và giữ nguyên các vlan trunking trước đó thì dùng câu lệnh:*

(config-if)# switchport trunk allowed vlan add <vlan-list>

+***Với Juniper Junos:***

<hostname> set interface <interface-name> unit 0 family ethernet-switching vlan members <vlan-id khác>

<hostname> set interface <interface-name> unit 0 family ethernet-switching vlan members <vlan-id khác>

+ Lệnh kiểm tra:

+***Với Cisco IOS:***

 # show running-config interface <trunk-port>

 # show interface trunk

 # show vlan brief

+***Với Cisco NX-OS:***

 # show running-config interface <trunk-port>

 # show interface trunk

 # show vlan brief

+***Với Juniper Junos:***

<hostname> show vlans

<hostname> show ethernet-switching interfaces

3.3. Cấu hình các giải pháp chống tấn công lớp 2.

- Cấu hình static mapping địa chỉ IP – địa chỉ MAC, port security, 802.1x

Đối với static mapping địa chỉ IP – địa chỉ MAC:

+ Lệnh cấu hình:

+***Với Cisco IOS:***

(config) # arp <ip address> <mac address> arpa

+ ***Với Cisco NX-OS:***

(config)# interface <interface-name>

(config-if)# ip arp <ip address> <mac address>

+ ***Với Juniper Junos:***

<hostname> set arp <ip_address> (mac | multicast-mac) <mac_address>

- Đối với IP đã được cấp thì ghi chính xác địa chỉ MAC
- Đối với IP còn trống thì điền địa chỉ MAC không hợp lệ để nếu có thiết bị dùng IP này sẽ không truy cập được.

+ Lệnh kiểm tra:

+ ***Với Cisco IOS:***

 # show arp

+ ***Với Cisco NX-OS:***

 # show arp

 # show running-config arp

 # show ip arp

+ ***Với Juniper Junos:***

<hostname> show arp

<u>Đối với Port-Security</u>

+ Lệnh cấu hình

+ ***Với Cisco IOS:***

(config)# interface <interface>

(config-if)# switchport port-security

//Cấu hình các địa chỉ MAC tĩnh trên port và cấu hình số lượng MAC tối đa bằng đúng số lượng khai tĩnh.

(config-if)# switchport port-security mac-address <mac-address>

(config-if)# switchport port-security maximum <number>

// Hoặc có thể cấu hình tự học MAC theo cơ chế sticky

(config-if)# switchport port-security mac-address sticky

(config-if)# switchport port-security maximum <number>

// Drop gói tin từ các MAC không hợp lệ

(config-if)# switchport port-security violation protect

+***Với Cisco NX-OS:***

(config)# interface <interface>

(config-if)# switchport port-security

//Cấu hình các địa chỉ MAC tĩnh trên port và cấu hình số lượng MAC tối đa bằng đúng số lượng khai tĩnh.

(config-if)# switchport port-security mac-address <mac-address>

(config-if)# switchport port-security maximum <number>

// Hoặc có thể cấu hình tự học MAC theo cơ chế sticky

(config-if)# switchport port-security mac-address sticky

(config-if)# switchport port-security maximum <number>

// Drop gói tin từ các MAC không hợp lệ

(config-if)# switchport port-security violation protect

+***Với Juniper Junos:***

//Cấu hình các địa chỉ MAC tĩnh trên port và cấu hình số lượng MAC tối đa bằng đúng số lượng khai tĩnh.

<hostname> set interface < interface-name > allowed-mac <mac-address>

<hostname> set interface < interface-name > mac-limit <number-mac>

<hostname> set interface < interface-name > vlan <vlan> mac-limit <number-mac>

// Hoặc có thể cấu hình tự học MAC theo cơ chế sticky

<hostname> set interface < interface-name > persistent-learning

// Drop gói tin từ các MAC không hợp lệ

<hostname> set interface < interface-name > mac-limit action drop

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show port-security

 # show running-config interface <interface>

+***Với Cisco NX-OS:***

 # show port-security

 # show running-config interface <interface>

 # show running-config port-security

+***Với Juniper Junos:***

<hostname> show ethernet-switching table

<u>Đối với xác thực 802.1x</u>

+ Lệnh cấu hình

+***Với Cisco IOS:***

// Cấu hình Radius server (primary và secondary)

(config)# radius-server host <ip-add> auth-port 1812 acct-port 1813 key <key>

// Bật xác thực dot1x qua radius

(config)# aaa authentication dot1x default group radius

(config)# aaa authorization network default group radius

(config)# dot1x system-auth-control

// Đặt chu kì re-authenticate

(config)# interface fa0/2

(config-if)# dot1x timeout reauth-period 86400

// Tắt tiến trình stpd trên các port thuộc vlan cấu hình 802.1x

(config)# no spanning-tree vlan <vlan-id>

// Bật tính năng netlogin dot1x mức port

(config)# interface fa0/2

(config-if)# authentication host-mode single-host|multi-host|multi-auth

(config-if)# authentication port-control auto

(config-if)# dot1x pae authenticator

+ ***Với Cisco NX-OS:***

// Cấu hình Radius server (primary và secondary)

(config)# radius-server host <ip-add> auth-port 1812 acct-port 1813 key <key>

// Bật xác thực dot1x qua radius

(config)# aaa authentication dot1x default group radius

(config)# aaa authorization network default group radius

(config)# dot1x system-auth-control

// Đặt chu kì re-authenticate

(config)# interface fa0/2

(config-if)# dot1x timeout re-authperiod 86400

// Tắt tiến trình stpd trên các port thuộc vlan cấu hình 802.1x

(config)# no spanning-tree vlan <vlan-id>

// Bật tính năng netlogin dot1x mức port

(config)# interface fa0/2

(config-if)# dot1x host-mode single-host|multi-host|multi-auth

(config-if)# dot1x port-control auto

(config-if)# dot1x pae authenticator

+ ***Với Juniper Junos:***

// Cấu hình Radius server (primary và secondary)

<hostname> set access radius-server <ip-add> secret <key>

<hostname> set access radius-server <ip-add2> secret <key>

// Bật xác thực dot1x qua radius

<hostname> set access profile <profile-name> authentication-order radius

<hostname> set access profile <profile-name> authentication-server [<ip-add> <ip-add2>]

// Bật tính năng netlogin dot1x mức port

<hostname> set authenticator interface <interface-name> supplicant multiple

// Đặt chu kì re-authenticate

<hostname> set authenticator interface <interface-name> reauthentication interval seconds

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show running-config

+***Với Cisco NX-OS:***

 # show running-config

 # show radius-server

 # show dot1x all

+***Với Juniper Junos:***

<hostname> show ethernet-switching table

<hostname> show dot1x interface <interface-name> detail

+ Cấu hình ARP Inspection
  + Lệnh cấu hình

+***Với Cisco IOS:***

// Enable ARP Inspection trên vlan

(config)# ip arp inspection vlan <vlan-id>

// Cấu hình cổng trust

(config)# interface <interface-id>

(config-if)# ip arp inspection trust

+***Với Cisco NX-OS:***

// Enable ARP Inspection trên vlan

(config)# ip arp inspection vlan <vlan-id>

// Cấu hình cổng trust

(config)# interface <interface-id>

(config-if)# ip arp inspection trust

+***Với Juniper Junos with ELS:***

<hostname> set vlans vlan-name forwarding-options dhcp-security arp-inspection

+***Với Juniper Junos non-ELS:***

<hostname> set ethernet-switching-options secure-access-port vlan vlan-name arp-inspection

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show ip arp inspection interfaces <interface-id>

 # show ip arp inspection vlan <vlan-id>

+***Với Cisco NX-OS:***

 # show ip arp inspection interfaces <interface-id>

 # show ip arp inspection vlan <vlan-id>

+***Với Juniper Junos:***

<hostname> show arp inspection statistics

- Cấu hình BPDU guard trên các port access

<u>Ngoại lệ:</u> Không cấu hình mục này đối với các port access kết nối với hệ thống ảo hóa (do hệ thống này có các switch ảo giả lập).

+ Lệnh cấu hình

+***Với Cisco IOS:***

(config)# interface <interface>

(config-if)# spanning-tree portfast

(config-if)# spanning-tree bpduguard enable

+***Với Cisco NX-OS:***

(config)# interface <interface>

(config-if)# spanning-tree port type edge

(config-if)# spanning-tree bpduguard enable

+***Với Juniper Junos:***

<hostname> set protocols rstp interface <interface-name> edge

<hostname> set protocols rstp bpdu-block-on-edge

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show spanning-tree interface <port> detail

 # show spanning-tree summary

+***Với Cisco NX-OS:***

 # show spanning-tree interface <port> detail

 # show spanning-tree summary

 # show running-config spanning-tree

+***Với Juniper Junos:***

<hostname> show spanning-tree interface

- Cấu hình Port-Isolate

<u>Ngoại lệ:</u> Không cấu hình mục này đối với các port cho máy in và gateway.

+ Lệnh cấu hình

+ ***Với Cisco IOS:***

(config)# interface <interface>

(config-if)# switchport protected

+ ***Với Juniper Junos:***

set vlans <user-vlan> no-local-switching

set vlans <user-vlan> interface <interface-gateway> pvlan-trunk

set vlans <user-vlan> interface <interface-user>

+ Lệnh kiểm tra

+ ***Với Cisco IOS:***

 # show interfaces <interface-name> switchport

+ ***Với Juniper Junos:***

<hostname> show vlans pvlan extensive

4. Cấu hình an ninh lớp 3

4.1. Yêu cầu xác thực cho các giao thức lớp 3

- VRRP, HSRP, GLBP, NSRP phải cấu hình xác thực cho giao thức giữa các thiết bị

Đối với HSRP

+ Lệnh cấu hình

+ ***Với Cisco IOS:***

// Thiết bị Master

(config)# interface vlan <vlan-id>

(config-if)# standby <id> priority 105

(config-if)# standby <id> ip <virtual-ip>

(config-if)# standby <id> preempt

(config-if)# standby <id> authentication <string>

// Thiết bị Standby

(config)# interface vlan <vlan-id>

(config-if)# standby <id> priority 95

(config-if)# standby <id> ip <virtual-ip>

(config-if)# standby <id> authentication <string>

+***Với Cisco NX-OS:***

// Thiết bị Master

(config)# interface vlan <vlan-id>

(config-if)# hsrp <id>

(config-if-hsrp)# priority 105

(config-if-hsrp)# ip <virtual-ip>

(config-if-hsrp)# preempt

(config-if-hsrp)# authenticate md5 key-chain <key-chain|key-string>

// Thiết bị Standby

(config)# interface vlan <vlan-id>

(config-if)# hsrp <id>

(config-if-hsrp)# priority 95

(config-if-hsrp)# ip <virtual-ip>

(config-if-hsrp)# authenticate md5 key-chain <key-chain|key-string>

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show standby

 # show running-config

+***Với Cisco NX-OS:***

 # show hsrp group <id>

 # show running-config

Đối với VRRP

+ Lệnh cấu hình

+***Với Cisco IOS:***

// Thiết bị Master

(config)# interface vlan <vlan-id>

(config-if)# vrrp <id> priority 105

(config-if)# vrrp <id> authentication <string>

(config-if)# vrrp <id> ip <virtual-ip>

(config-if)# vrrp <id> preempt delay minimum <seconds>

// Thiết bị Standby

(config)# interface vlan <vlan-id>

(config-if)# vrrp <id> priority 95

(config-if)# vrrp <id> authentication <string>

(config-if)# vrrp <id> ip <virtual-ip>

+***Với Cisco NX-OS:***

// Thiết bị Master

(config)# interface vlan <vlan-id>

(config-if)# vrrp <id>

(config-if-vrrp)# priority 105

(config-if-vrrp)# address <virtual-ip>

(config-if-vrrp)# authentication text <string>

// Thiết bị Standby

(config)# interface vlan <vlan-id>

(config-if)# vrrp <id>

(config-if-vrrp)# priority 95

(config-if-vrrp)# address <virtual-ip>

(config-if-vrrp)# authentication text <string>

+***Với Juniper Junos:***

// Thiết bị Master

<hostname> set interfaces <interface-name> unit 0 family inet address <IP1> vrrp-group 1 virtual-address <VIP>

<hostname> set interfaces <interface-name> unit 0 family inet address <IP1> vrrp-group 1 authentication-type md5

<hostname> set interfaces <interface-name> unit 0 family inet address <IP1> vrrp-group 1 authentication-key <key>

<hostname> set interfaces <interface-name> unit 0 family inet address <IP1> vrrp-group 1 accept-data

<hostname> set interfaces <interfaces> unit 0 family inet address <IP1> vrrp-group 1 track interface <interface-name> priority-cost 200

// Thiết bị Standby

<hostname> set interfaces <interface-name> unit 0 family inet address <IP2> vrrp-group 1 virtual-address <VIP>

<hostname> set interfaces <interface-name> unit 0 family inet address <IP2> vrrp-group 1 authentication-type md5

<hostname> set interfaces <interface-name> unit 0 family inet address <IP2> vrrp-group 1 authentication-key <key>

<hostname> set interfaces <interface-name> unit 0 family inet address <IP2> vrrp-group 1 accept-data

<hostname> set interfaces <interfaces> unit 0 family inet address <IP1> vrrp-group 1 track interface <interface-name> priority-cost 100

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show vrrp brief

 # show running-config

+***Với Cisco NX-OS:***

 # show vrrp

 # show running-config

+***Với Juniper Junos:***

<hostname> show vrrp

<u>Đối với GLBP</u>

+ Lệnh cấu hình

+***Với Cisco IOS:***

// Thiết bị Master

(config)# interface vlan <vlan-id>

(config-if)# glbp <id> ip <virtual-ip>

(config-if)# glbp <id> priority 105

(config-if)# glbp <id> authentication md5 key-string <string>

(config-if)# glbp <id> preempt delay minimum <seconds>

// Thiết bị Standby

(config)# interface vlan <vlan-id>

(config-if)# glbp <id> ip <virtual-ip>

(config-if)# glbp <id> priority 95

(config-if)# glbp <id> authentication md5 key-string <string>

+***Với Cisco NX-OS:***

// Thiết bị Master

(config)# interface vlan <vlan-id>

(config-if)# glbp <id>

(config-if-glbp)# priority 105

(config-if-glbp)# ip <virtual-ip>

(config-if-glbp)# authentication md5 key-string <string>

(config-if-gblbp)# preempt delay minimum <seconds>

// Thiết bị Standby

(config)# interface vlan <vlan-id>

(config-if)# glbp <id>

(config-if-glbp)# priority 95

(config-if-glbp)# ip <virtual-ip>

(config-if-glbp)# authentication md5 key-string <string>

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show glbp <id>

 # show running-config

+***Với Cisco NX-OS:***

 # show glbp <id>

 # show running-config

- OSPF phải thiết lập chuỗi xác thực có mã hóa giữa 2 thiết bị

+ Lệnh cấu hình

+***Với Cisco IOS:***

//Enable xac thuc giua 2 thiet bi neighbor voi nhau

(config)# interface <interface-name>

(config-if)# no switchport

(config-if)# ip ospf message digest-key <keyid> md5 <key> <password>

(config-if)# ip ospf authentication message-digest

//Enable xac thuc giua cac thiet bi trong cung area

(config)# interface <interface-name>

(config-if)# no switchport

(config-if)# ip ospf message digest-key <keyid> md5 <password>

(config-if)# exit

(config)# router ospf process-id

(config-router)# area area-id authentication message-digest

(config-router)# exit

Với Cisco NX-OS:

//Enable xac thuc giua 2 thiet bi neighbor voi nhau

(config)# interface <interface-name>

(config-if)# no switchport

(config-if)# ip ospf message digest-key <keyid> md5 <key> <password>

(config-if)# ip ospf authentication message-digest

//Enable xac thuc giua cac thiet bi trong cung area

(config)# interface <interface>

(config-if)# no switchport

(config-if)# ip ospf message digest-key <keyid> md5 <key> <password>

(config-if)# exit

(config)# router ospf process-id

(config-router)# area area-id authentication message-digest

(config-router)# exit

+***Với Juniper Junos:***

//Enable xac thuc giua 2 thiet bi neighbor voi nhau

<hostname> set protocols ospf area 0.0.0.0 interface <interface_name> authentication md5 1 key <password>

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show ip ospf interface <interface-name>

 # show ip ospf neighbor

+***Với Cisco NX-OS:***

 # show ip ospf interface <interface-name>

 # show ip ospf neighbor

+***Với Juniper Junos:***

<hostname> show protocols ospf

- BGP phải thiết lập chuỗi xác thực có mã hóa giữa các peer

+ Lệnh cấu hình

+***Với Cisco IOS:***

(config)# router bgp <AS-number>

(config-router)# neighbor <ip-address> password <password>

+***Với Cisco NX-OS:***

(config)# router bgp 65536

(config-router)# neighbor <ip address> remote-as <remote-AS>

(config-router-neighbor)# password <password>

+***Với Juniper Junos:***

<hostname> set protocols bgp group <BGP_Group> type external

<hostname> set protocols bgp group <BGP_Group> peer-as <Neighbor_AS>

<hostname> set protocols bgp group <BGP_Group> neighbor <Neighbor_ip>

<hostname> set routing-options autonomous-system <AS>

<hostname> set protocols bgp group <BGP_Group> authentication-key-chain <BGP_chain_password>

<hostname> set protocols bgp group <BGP_Group> authentication-algorithm md5

<hostname> set security authentication-key-chains key-chain <BGP_chain_password> tolerance 30

<hostname> set security authentication-key-chains key-chain <BGP_chain_password> key 0 secret <password>

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show running-config

 # show ip bgp summary

+***Với Cisco NX-OS:***

 # show running-config

 # show ip bgp neighbor

+***Với Juniper Junos:***

<hostname> show protocols bgp

- Các quy tắc thiết lập chuỗi xác thực giữa các giao thức lớp 3, người quản trị khi thiết lập cấu hình cần tuân theo:

+ Có độ phức tạp bao gồm chữ in thường, in hoa, ký tự đặc biệt
+ Chuỗi dài hơn 10 ký tự
+ Không đặt các mật khẩu dễ đoán

4.2. Yêu cầu kiểm soát định tuyến chính xác.

- Với các giao thức định tuyến động: Thực hiện chặn quảng bá thông tin định tuyến ra ngoài các port không cần thiết (Port đấu xuống khách hàng, thiết bị đầu cuối...)

+ Lệnh cấu hình

+***Với Cisco IOS:***

//OSPF:

(config)# router ospf <Process_ID>

(config-router)# passive-interface <interface-name>

//EIGRP

(config)# router eigrp {autonomous-system-number | virtual-instance-number}

(config-router)# passive-interface <interface-name>

//IS-IS

(config)# router isis

(config-router)# passive-interface <interface-name>

+***Với Cisco NX-OS:***

//OSPF

(config)# interface <interface-name }

(config-if)# {ip | ipv6} ospf passive-interface

//EIGRP

(config)# interface <interface-name }

(config-if)# {ip | ipv6} passive-interface eigrp

//IS-IS

(config)# interface <interface-name }

(config-if)# isis passive { level-1 | level-2 | level-1-2 }

+***Với Juniper Junos:***

//OSPF

set protocols ospf area <ID> interface <interface-name> passive

//IS-IS

set protocols isis interface <interface-name> passive

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show ip eigrp interfaces

 # show ip ospf interfaces

 # show ip isis interfaces

+***Với Cisco NX-OS:***

 # show { ip | ipv6 } eigrp [instance-tag] interfaces [brief] [detail]

 # show ip ospf interface

 # show isis [instance-tag] interface [brief

+***Với Juniper Junos:***

<hostname> show protocol ospf

<hostname> show protocol isis

<hostname> show isis interface

<hostname> show ospf interface

4.3. Yêu cầu tách bảng định tuyến giữa lớp dịch vụ và lớp giám sát thông qua VRF riêng

- Thiết bị switch layer 3, router có các interface đấu public phải tách bảng định tuyến giữa lớp dịch vụ và lớp giám sát thông qua VRF riêng cho lưu lượng OAM (với trường hợp lớp giám sát không đi qua Firewall)

+ Lệnh cấu hình

+***Với Cisco IOS:***

//Tạo VRF:

(config)# ip vrf <vrf-name>

//Đưa interface giám sát vào VRF

(config)# interface <interface-name>

(config-if)# ip vrf forwarding <vrf-name>

(config-if)# ip address <IP> <subnet mask>

+***Với Cisco NX-OS:***

//Tạo VRF:

(config)# vrf context <vrf-name>

//Đưa interface giám sát vào VRF

(config)# interface <interface-name>

(config-if)# vrf member <vrf-name>

(config-if)# ip address <IP/subnetmask>

+***Với Juniper Junos:***

//Tạo VRF:

<hostname> set routing-instances <vrf-name> instance-type virtual-router

//Đưa interface giám sát vào VRF

<hostname> set routing-instances <vrf-name> interface <interface-name>

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show running-config

 # show running-config vrf

+***Với Cisco NX-OS:***

 # show running-config

 # show vrf

+***Với Juniper Junos:***

<hostname> show route instance

4.4. Yêu cầu bật tính năng DHCP Snooping

- Mạng văn phòng sử dụng DHCP cho máy tính người dùng phải bật tính năng DHCP Snooping trên các port access

+ Lệnh cấu hình

+***Với Cisco IOS:***

//Enable mức global

(config)# ip dhcp snooping

//Enable cho 1 vlan cu the (vlan client)

(config)# ip dhcp snooping vlan <vlan-id>

//Neu 1 port trong vlan da enable dhcp snooping co ket noi voi dhcp server thi enable trust cho port nay

(config)# interface <interface-name>

(config-if)#ip dhcp snooping trust

Với Cisco NX-OS:

//Enable mức global

(config)# ip dhcp snooping

//Enable cho 1 vlan cu the (vlan client)

(config)# ip dhcp snooping vlan <vlan-id>

//Neu 1 port trong vlan da enable dhcp snooping co ket noi voi dhcp server thi enable trust cho port nay

(config)# interface <interface-name>

(config-if)#ip dhcp snooping trust

+***Với Juniper Junos:***

//Enable muc global

<hostname> set vlan all examine-dhcp

//Enable cho 1 vlan cu the (vlan client)

<hostname> set vlan <vlan-id> examine-dhcp <vlan-id>

//Neu 1 port trong vlan da enable dhcp snooping co ket noi voi dhcp server thi enable trust cho port nay

<hostname> set interface <interface-name> dhcp-trusted

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show ip dhcp snooping

Với Cisco NX-OS:

 # show ip dhcp snooping

 # show running-config dhcp

+***Với Juniper Junos:***

<hostname> show dhcp snooping binding

5. Về cấu hình quản trị

5.1. Yêu cầu về sao lưu cấu hình

- Lưu cấu hình trước khi tác động và định kì tối thiểu 01 lần/quý. Lưu tối thiểu 02 bản gần nhất. Không lưu bản sao lưu trên máy tính cá nhân của quản trị viên

+ Lệnh cấu hình

+***Với Cisco IOS:***

(config)# kron policy-list backup

(config-kron-policy)# cli show run | redirect tftp://10.1.1.1/test.cfg

(config-kron-policy)# exit

(config)# kron occurrence backup at 23:00 Sun recurring

(config-kron-occurrence)# policy-list backup

Với Cisco NX-OS:

(config)# feature scheduler

(config)# scheduler job name backup-daily

(config-job)# copy running-config tftp:// 10.1.1.1/$(SWITCHNAME)-cfg.$(TIMESTAMP)

(config-job)# exit

(config)# scheduler schedule name backup-daily

(config-schedule)# time weekly Sun:23:00

(config-schedule)# job name backup-daily

+***Với Juniper Junos:***

<hostname> set system archival configuration transfer-on-commit

<hostname> set system archival configuration transfer-interval interval

<hostname> set system archival configuration archive-sites <ftp-link>

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show running-config

Với Cisco NX-OS:

 # show running-config

 # show scheduler config

+***Với Juniper Junos:***

<hostname> show configuration

5.2. Yêu cầu về quản lý tài khoản

- Khuyến nghị sử dụng hệ thống AAA để quản lý tài khoản người dùng tập trung (xác thực, phân quyền, ghi lịch sử tác động). Tối đa 02 tài khoản quản trị local dùng cho trường hợp khẩn cấp

+ Lệnh cấu hình:

+ ***Với Cisco IOS:***

(config)# aaa new-model

(config)# tacacs-server host 10.1.1.1

(config)# tacacs-server key <tacacs-shared-key>

// Xác thực truy nhập user mode

(config)# aaa authentication login default group TACACS+ local

// Xác thực truy nhập enable mode

(config)# aaa authentication enable default group TACACS+ enable

// Phân quyền cho phép user xác thực thành công sẽ có thể thực thi tất cả câu lệnh cấu hình trong config mode nhưng không back được lại enable mode để thực thi shutdown…

(config)# aaa authorization config-commands

// Phân quyền cho phép user xác thực thành công sẽ có thể nhảy vào lần lượt từng exec mode

(config)# aaa authorization exec default group TACACS+ local if-authenticated

// Phân quyền theo từng privilege level của user

(config)# aaa authorization commands 10 default group TACACS+ if-authenticated

// Cấu hình accounting

(config)# aaa accounting exec default start-stop group TACACS+

(config)# aaa accounting commands 1 default start-stop group TACACS+

(config)# aaa accounting commands 15 default start-stop group TACACS+

// Tạo account admin local

(config)# username admin1 privilege 15 password <password>

(config)# username admin2 privilege 15 password <password>

+ ***Với Cisco NX-OS:***

(config)# tacacs-server host 10.1.1.1

(config)# tacacs-server key 7 <tacacs-shared-key>

// Xác thực truy nhập user mode

(config)# aaa authentication login default group TACACS+ local

// Phân quyền cho phép user xác thực thành công sẽ có thể thực thi tất cả câu lệnh cấu hình trong config mode nhưng không back được lại enable mode để thực thi shutdown…

(config)# aaa authorization config-commands default group TACACS+ local

// Phân quyền cho phép user xác thực thành công sẽ có thể nhảy vào lần lượt từng exec mode

(config)# aaa authorization exec default group TACACS+ local if-authenticated

// Phân quyền theo từng privilege level của user

(config)# aaa authorization commands default group TacServer local

// Cấu hình accounting

(config)# aaa accounting default group TACACS+ local

// Tạo account admin local

(config)# username admin1 password 5 <password> role <role-name>

(config)# username admin2 password 5 <password> role <role-name>

+ ***Với Juniper Junos:***

<hostname> set system tacplus-server <tacac_server> timeout 5

<hostname> set system tacplus-server <tacac_server> secret <password>

<hostname> set system tacplus-server <tacac_server> source-address <ip>

<hostname> set system tacplus-server <tacac_server> port <port-number>

// Xác thực truy nhập user mode

<hostname> set system authentication-order tacplus

<hostname> set system authentication-order password

// Cấu hình accounting

<hostname> set system accounting destination tacplus server <tacac_server> port <port-number>

<hostname> set system accounting destination tacplus server <tacac_server> source-address <ip>

+ Lệnh kiểm tra

+ ***Với Cisco IOS:***

 # show running-config

Với Cisco NX-OS:

 # show running-config

+***Với Juniper Junos:***

<hostname> show configuration

+ Quản trị viên phải sử dụng tài khoản được cấp riêng, phân quyền phù hợp trên local/AAA

<u>Đối với tài khoản Local</u>

+ Lệnh cấu hình

+***Với Cisco IOS:***

// Tạo account admin local

(config)# username admin1 privilege 15 password <password>

(config)# username admin2 privilege 15 password <password>

// Xóa account local không sử dụng

(config)# no username <username>

Với Cisco NX-OS:

// Tạo account admin local

(config)# username admin1 password 5 <password> role <role-name>

(config)# username admin2 password 5 <password> role <role-name>

// Xóa account local không sử dụng

(config)# no username <username>

+***Với Juniper Junos:***

// Tạo account admin local

<hostname> set system login user admin1

<hostname> set system login user admin1 class super-user

<hostname> set system login user admin1 authentication encrypted-password

// Xóa account local không sử dụng

<hostname> delete system login user adminx

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show running-config

+ ***Với Cisco NX-OS:***

 # show running-config

+ ***Với Juniper Junos:***

<hostname> show configuration | display set | match user

<u>Đối với tài khoản AAA</u>

+ Kiểm tra tài khoản, phân quyền trên AAA Server.

- Đổi mật khẩu mặc định các tài khoản local của thiết bị

+ Lệnh cấu hình

+ ***Với Cisco IOS:***

// Tượng tự lệnh tạo account admin local

(config)# username admin privilege 15 password <mypassword>

+ ***Với Cisco NX-OS:***

// Tượng tự lệnh tạo account admin local

(config)# username admin password 5 <password> role <role-name>

+ ***Với Juniper Junos:***

// Tượng tự lệnh tạo account admin local

<hostname> set system login user admin1 authentication encrypted-password

+ Lệnh kiểm tra

+ ***Với Cisco IOS:***

 # show running-config

+ ***Với Cisco NX-OS:***

 # show running-config

+ ***Với Juniper Junos:***

<hostname> show configuration | display set | match user

- Thiết lập chính sách mật khẩu mạnh cho các tài khoản trên local/AAA, ẩn đi trên cấu hình:

+ Yêu cầu có độ phức tạp bao gồm chữ in thường, in hoa, ký tự

+ Mật khẩu dài hơn 10 ký tự

+ Không đặt các mật khẩu dễ đoán

Khóa sau 5 lần đăng nhập sai, thời gian khóa tài khoản do đăng nhập sai là 10 phút

Đối với account local

*- Lưu ý: Từ Cisco IOS 12.3(14) trở lên có tùy chọn sẽ khóa tài khoản nếu đăng nhập sai quá số lần quy định. Tuy nhiên với những user có privilege 15 sẽ kh*ông *bị ảnh hưởng bởi tùy chọn này.*

+ Lệnh cấu hình (Cisco IOS 12.3 trở lên)

+***Với Cisco IOS:***

(config)# aaa new-model

(config)# aaa local authentication attempts max-fail 5

//Để unlock 1 user bị khóa thì dùng lệnh sau:

 # clear aaa local user fail-attempts username <USERNAME>

// Mã hóa tất cả mật khẩu trong file cấu hình sử dụng kiểu mã hóa 7 của Cisco

(config)#service password-encryption

+***Với Cisco NX-OS:***

(config)# aaa authentication rejected 10 in 100 ban 600

//Để unlock 1 user bị khóa thì dùng lệnh sau:

 # clear aaa local user blocked <USERNAME>

Mặc định thì NX-OS tự động mã hóa tất cả mật khẩu khai báo trên cấu hình

+***Với Juniper Junos:***

<hostname> set retry-options lockout-period 5

<hostname> set retry-options tries-before-disconnect 10

<hostname> set system login password minimum-length 12

<hostname> set system login password maximum-length 22

<hostname> set system login password minimum-numerics 1

<hostname> set system login password minimum-upper-cases 1

<hostname> set system login password minimum-lower-cases 1

<hostname> set system login password minimum-punctuations 1

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show aaa local user lockout

 # show running-config

+***Với Cisco NX-OS:***

 # show aaa local user blocked

 # show running-config

*+**Với Juniper Junos:***

<hostname> show system login lockout

<hostname> show system login password

<u>Đối với account AAA</u>

+ Cấu hình và kiểm tra chính sách mật khẩu trên AAA Server.

5.3. Yêu cầu về kết nối quản trị

- Khuyến nghị quản trị thiết bị qua VLAN quản trị dành riêng

+ Lệnh cấu hình

*+**Với Cisco IOS:***

(config)# vlan <mgmt-vlan-id>

(config-vlan)# name VLAN_MGMT

(config-vlan)# exit

(config)# interface vlan <mgmt-vlan-id>

(config-if)# ip address <ip> <mask>

(config-if)# exit

(config)# interface <interface-name>

(config-if)# switchport mode access

(config-if)# switchport access vlan <mgmt-vlan-id>

*+**Với Cisco NX-OS:***

(config)# vlan <mgmt-vlan-id>

(config-vlan)# name VLAN_MGMT

(config-vlan)# exit

(config)# feature interface-vlan

(config)# interface vlan <mgmt-vlan-id>

(config-if)# ip address <ip/length>

(config-if)# exit

(config)# interface <interface-name>

(config-if)# switchport mode access

(config-if)# switchport access vlan <mgmt-vlan-id>

*+**Với Juniper Junos:***

<hostname> set vlans <vlan-name> description <vlan-description>

<hostname> set vlans <vlan-name> vlan-id < mgmt-vlan-id >

<hostname> set vlans <vlan-name> l3-interface <vlan-name>

<hostname> set interfaces vlan unit <mgmt-vlan-id> family inet address <ip-address>

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show interface vlan <mgmt-vlan-id>

+***Với Cisco NX-OS:***

 # show interface vlan <mgmt-vlan-id>

+***Với Juniper Junos:***

<hostname> show interface vlan <mgmt-vlan-id>

- Quản trị thiết bị qua kết nối trực tiếp Console hoặc kết nối từ xa an toàn, có mã hóa (SSHv2, HTTPS). Tắt các giao thức quản trị từ xa không an toàn (Telnet, HTTP)

- Thời gian time-out của các phiên kết nối quản trị tối đa là 15 phút.

- Giới hạn chỉ cho phép quản trị từ các IP theo danh sách đăng kí

Cấu hình Console

+ Lệnh cấu hình

+***Với Cisco IOS:***

(config)#line console 0

(config-line)#login authentication default

(config-line)#exec-timeout 15

+***Với Cisco NX-OS:***

(config)#line console 0

(config-line)#exec-timeout 15

+***Với Juniper Junos:***

<hostname> set console authentication-order password

+ Lệnh kiểm tra

+***Với Cisco IOS:***

(config)# show running-config

+***Với Cisco NX-OS:***

(config)# show running-config

+ ***Với Juniper Junos:***

<hostname> show configuration

<u>Cấu hình SSH</u>

+ Lệnh cấu hình

+ ***Với Cisco IOS:***

// Tạo key RSA cho SSH

(config)#ip domain-name tct.com

(config)#crypto key generate rsa general-keys modulus 1024

// Tạo access-list giới hạn các IP nguồn được phép quản trị thiết bị

(config)#access-list 1 permit 192.168.1.1

(config)#access-list 1 permit 192.168.1.2

// Chỉ cho phép SSH, không cho phép Telnet, giới hạn ip quản trị bằng ACL, đặt time-out

(config)#no ip http server

(config)#line vty 0 4

(config-line)#login authentication default

(config-line)#transport input ssh

(config-line)#access-class 1 in

(config-line)#exec-timeout 15

+ ***Với Cisco NX-OS:***

// Tạo key RSA cho SSH

(config)#ip domain-name tct.com

Mặc định NX-OS đã bật sẵn SSHv2 và khởi tạo RSA key 1024 bit. Nếu muốn khởi tạo lại RSA key khác theo chính sách riêng của công ty thì thực hiện lệnh:

(config)#no feature ssh

(config)#ssh key rsa <bits>

(config)#feature ssh

// Tạo access-list giới hạn các IP nguồn được phép quản trị thiết bị

(config)#access-list 1 permit 192.168.1.1

(config)#access-list 1 permit 192.168.1.2

// Chỉ cho phép SSH, không cho phép Telnet, giới hạn ip quản trị bằng ACL, đặt time-out

(config)#no feature http-server

(config)#no feature telnet

(config)#line vty 0 4

(config-line)#ip access-class 1 in

(config-line)#exec-timeout 15

+***Với Juniper Junos:***

// Enable dịch vụ ssh

<hostname> set system services ssh root-login deny

<hostname> set system services ssh protocol-version v2

// Tạo access-list giới hạn các IP nguồn được phép quản trị thiết bị

<hostname> set policy-options prefix-list <ssh-list> <ip1>

<hostname> set policy-options prefix-list <ssh-list> <ip2>

<hostname> set policy-options prefix-list <ssh-list> <ip3>

// Chỉ cho phép SSH, không cho phép Telnet, giới hạn ip quản trị bằng ACL, đặt time-out

<hostname> set interfaces <mgmt_interface> unit 0 family inet filter input <name_filter>

(set firewall family inet filter <name_filter> term SSH_TELNET from source-prefix-list <ssh-list>

<hostname> set firewall family inet filter <name_filter> term <ssh-list> from protocol tcp <hostname> set firewall family inet filter <name_filter> term <ssh-list> from port ssh <hostname> set firewall family inet filter <name_filter> term <ssh-list> then count SSH <hostname> set firewall family inet filter <name_filter> term <ssh-list> then accept

+ Lệnh kiểm tra

+***Với Cisco IOS:***

(config)# show running-config

+***Với Cisco NX-OS:***

(config)# show running-config

+***Với Juniper Junos:***

<hostname> show configuration

<u>Cấu hình HTTPS</u>

+ Lệnh cấu hình

+ ***Với Cisco IOS:***

(config)#ip http secure-server

(config)#ip http authentication aaa

(config)#ip http access-class 1

(config)#ip http timeout-policy idle 900

+ ***Với Cisco NX-OS:***

(config)#no feature http-server

(config)#feature nxapi

(config)#no nxapi http

+ ***Với Juniper Junos:***

<hostname> set system services web-management https interface <mgmt_interface>

<hostname> set system services web-management https system-generated-certificate

+ Lệnh kiểm tra

+ ***Với Cisco IOS:***

(config)# show running-config

+ ***Với Cisco NX-OS:***

(config)# show running-config

+ ***Với Juniper Junos:***

<hostname> show configuration

5.4. Yêu cầu cấu hình NTP

- Đồng bộ thời gian theo tối thiểu 01 máy chủ thời gian (NTP server)

+ Lệnh cấu hình:

+ ***Với Cisco IOS:***

(config)#clock timezone HaNoi 7

(config)#ntp server 192.168.181.50

(config)#ntp server 203.113.131.70

(config)#ntp source-interface <interface>

+ ***Với Cisco NX-OS:***

(config)#clock timezone HaNoi 7 0

(config)#ntp server 192.168.181.50 prefer

(config)#ntp server 203.113.131.70

(config)#ntp source-interface <interface>

+***Với Juniper Junos:***

<hostname> set system time-zone Asia/Saigon

<hostname> set system ntp server <ip-ntp-server> prefer

+ Lệnh kiểm tra

+***Với Cisco IOS:***

#show ntp associations

#show ntp status

+***Với Cisco NX-OS:***

#show ntp associations

#show ntp peers

#show ntp peer-status

+***Với Juniper Junos:***

<hostname> show ntp status

5.5. Yêu cầu cấu hình log

- Thiết bị phải được thiết lập bật chế độ ghi log và cấu hình lưu log tập trung tối thiểu 06 tháng cho các hệ thống cấp độ 3 theo quy định của bộ Thông tin Truyền thông. Trong trường hợp không có hệ thống lưu log tập trung thực hiện thiết lập lưu trên local

+ Lệnh cấu hình:

+***Với Cisco IOS:***

(config)#logging on

(config)#logging [trap | console | history | monitor] [level]

(config)#logging host <syslog-server-ip>

(config)#logging source-interface vlan <vlan-id>

(config)#logging count

(config)#logging userinfo

// Cấu hình timestamps trong các bản tin log

(config)#service timestamps debug datetime localtime show-timezone msec year

(config)#service timestamps log datetime localtime show-timezone msec year

+ ***Với Cisco NX-OS:***

(config)#logging [trap | console | history | monitor] [level]

(config)#logging host <syslog-server-ip>

(config)#logging source-interface vlan <vlan-id>

+ ***Với Juniper Junos:***

<hostname> set system syslog archive size 10m

<hostname> set system syslog archive files 10

*<hostname> set system syslog user * any critical*

<hostname> set system syslog host <log_server> any notice

<hostname> set system syslog host <log_server> daemon any

<hostname> set system syslog host <log_server> kernel any

<hostname> set system syslog host <log_server> interactive-commands any

<hostname> set system syslog host <log_server> facility-override local7

<hostname> set system syslog host <log_server> any notice

<hostname> set system syslog file messages any warning

<hostname> set system syslog file messages authorization none

<hostname> set system syslog file messages archive world-readable

<hostname> set system syslog file messages explicit-priority

<hostname> set system syslog file interactive-commands interactive-commands any

<hostname> set system syslog file interactive-commands match "!(UI_JUNOSCRIPT_CMD)"

<hostname> set system syslog file security authorization any

<hostname> set system syslog file firewall-filter-log firewall any

<hostname> set system syslog file default-log-messages any any

<hostname> set system syslog file default-log-messages structured-data

<hostname> set system syslog file config-changes change-log info

<hostname> set system syslog console any alert

<hostname> set system syslog time-format year

<hostname> set system syslog time-format millisecond

<hostname> set system syslog source-address <ip_source>

+ Lệnh kiểm tra

+ ***Với Cisco IOS:***

 # show logging

 # show running-config

+ ***Với Cisco NX-OS:***

 # show running-config

(config)# show logging monitor

+ ***Với Juniper Junos:***

<hostname> show configuration

5.6. Yêu cầu cấu hình SNMP

- SNMP phiên bản v2c, v3
- SNMP theo chế độ read-only
- Community string SNMP riêng
- Xóa bỏ community string mặc định
- Chỉ cho phép truy cập SNMP từ máy chủ giám sát

Cấu hình cho tất cả các quy tắc trên:

<u>Với SNMP v2c</u>

+ Lệnh cấu hình

+ ***Với Cisco IOS:***

(config)# access-list <acl-number> permit <ip>

(config)# no snmp-server community public

(config)# no snmp-server community private

(config)# snmp-server community mystring ro <acl-number>

+ ***Với Cisco NX-OS:***

(config)# access-list <acl-number> permit <ip>

(config)# no snmp-server community public

(config)# no snmp-server community private

(config)# snmp-server community mystring ro

(config)# snmp-server community mystring use-acl <acl-number>

+ ***Với Juniper Junos:***

<hostname> set snmp client-list <NMS-SRV> <Ip1> <hostname> set snmp client-list <NMS-SRV> <Ip2>

<hostname> set snmp community <ComPrivate> authorization read-only
<hostname> set snmp community < ComPrivate> client-list-name <NMS-SRV>

+ Lệnh kiểm tra

+***Với Cisco IOS:***

 # show snmp

 # show snmp community

 # show running-config

+***Với Cisco NX-OS:***

 # show snmp

 # show snmp community

 # show running-config

+***Với Juniper Junos:***

<hostname> show snmp statistics

<hostname> show configuration

<u>Với SNMP v3</u>

+ Lệnh cấu hình

+***Với Cisco IOS:***

(config)# access-list <acl-number> permit <ip>

(config)# snmp-server view TestSNMPv3View internet included

(config)# snmp-server group TestSNMPv3Group v3 priv read TestSNMPv3View

(config)# snmp-server user TestSNMPv3User TestSNMPv3Group v3

auth [md5 | sha] mypassword priv [des56 | aes] mypassword access <acl-number>

+***Với Cisco NX-OS:***

(config)# access-list <acl-number> permit <ip>

(config)# snmp-server view TestSNMPv3View internet included

(config)# snmp-server group TestSNMPv3Group v3 priv read TestSNMPv3View

(config)# snmp-server user TestSNMPv3User TestSNMPv3Group v3

auth [md5 | sha] mypassword priv [des56 | aes] mypassword access <acl-number>

+ ***Với Juniper Junos:***

<hostname> set snmp view <view-name> oid object-identifier include <obj>

<hostname> set snmp view

<hostname> set snmp v3 usm local-engine user <username-snmp>

<hostname> set snmp v3 usm local-engine user <username-snmp> authentication-md5 authentication-password authentication-password

<hostname> set snmp v3 usm local-engine user <username-snmp> privacy-des <privacy-password> <privacy-password>

+ Lệnh kiểm tra

+ ***Với Cisco IOS:***

 # show snmp view

 # show snmp user

 # show snmp group

 # show running-config

+ ***Với Cisco NX-OS:***

 # show snmp user

 # show snmp group

 # show running-config

+ ***Với Juniper Junos:***

<hostname> show snmp